FINANCE AND PERSONNEL COMMITTEE MEETING AGENDA

October 28, 2024 at 5:00 PM

Council Chambers, 828 Center Avenue, Sheboygan, WI

It is possible that a quorum (or a reverse quorum) of the Sheboygan Common Council or any other City committees/boards/commissions may be in attendance, thus requiring a notice pursuant to State ex rel. Badke v. Greendale Village Board, 173 Wis. 2d 553,494 N.W.2d 408 (1993).

Persons with disabilities who need accommodations to attend this meeting should contact the Finance Department at 920-459-3311. Persons other than council members who wish to participate remotely shall provide notice to the Finance Department at 920-459-3311 at least 24 hours before the meeting so that the person may be provided a remote link for that purpose.

OPENING OF MEETING

1. Call to Order
2. Roll Call - Alderperson Felde may attend remotely
3. Pledge of Allegiance
4. Introduction of Committee Members and Staff

MINUTES

5. Approval of Minutes - October 14, 2024

ITEMS FOR DISCUSSION AND POSSIBLE ACTION

6. Res. No. 105-24-25 / October 21, 2024: A RESOLUTION amending the 2024 budget for various expenses incurred or planned.
7. Res. No. 109-24-25 / October 21, 2024: A RESOLUTION approving City of Sheboygan Health Insurance Portability and Accountability Act (HIPAA Policies).

DATE OF NEXT REGULAR MEETING

8. Next Meeting Date - November 11, 2024

ADJOURN

9. Motion to Adjourn

In compliance with Wisconsin's Open Meetings Law, this agenda was posted in the following locations more than 24 hours prior to the time of the meeting:

City Hall • Mead Public Library
Sheboygan County Administration Building • City's website

CITY OF SHEBOYGAN
RESOLUTION 105-24-25

BY ALDERPERSONS MITCHELL AND PERRELLA.

OCTOBER 21, 2024.

A RESOLUTION amending the 2024 budget for various expenses incurred or planned.

RESOLVED: That the Finance Director is authorized to make amendments in the 2024 budget for the following:

Purchase of marina work boat and associated registration fees

INCREASE:	
Capital Fund – Public Works - Vehicles	$45,500
(Acct. No. 400300-651100)	
Capital Fund – Fund Equity Applied	$45,500
(Acct. No. 400-493000)	

Parts and labor for significant repairs to Fire Truck 1862

INCREASE:	
General Fund – Fire Department – Vehicle Maintenance & Repairs	$35,770
(Acct. No. 101220-562110)	
DECREASE:	
General Fund – City Administration – Contingency	$35,770
(Acct. No. 101141-810101)	

Electrical work at Fire Station #2 previously budgeted in 2022 with completion in 2024

INCREASE:	
Capital Fund – Public Safety – Building Improvements	$43,973
(Acct. No. 400200-631200)	
Capital Fund – Fund Equity Applied	$43,973
(Acct. No. 400-493000)	

Purchase of office furniture for additional Attorney

INCREASE:	
General Fund – City Attorney – Tools & Small Equipment	$7,918
(Acct. No. 101130-560255)	
DECREASE:	
General Fund – City Attorney – Full Time Salaries Regular	
(Acct. No. 101130-510110)	$7,918

Legal expenses in Human Resources due to union negotiations and personnel investigations

INCREASE:	
General Fund – Human Resources – Legal Services	$125,000
(Acct. No. 101144-531200)	
DECREASE:	
General Fund – City Administration – Contingency	$125,000
(Acct. No. 101141-810101)	

Contract with BoldPath Consulting for Department of Public Works department structure review

INCREASE:	
General Fund – Human Resources – Contracted Services	$36,000
(Acct. No. 101144-531100)	
DECREASE:	
General Fund – City Administration – Contingency	$36,000
(Acct. No. 101141-810101)	

Correct budget in TID 21 from Buildings to Land account for Wells Fargo Purchase due to best accounting practice

INCREASE:	
TID 21 Fund – Land	$1,700,000
(Acct. No. 421660-621100)	
DECREASE:	
TID 21 Fund – Buildings	$1,700,000
(Acct. No. 421660-631100)	

Purchase of Sheboygan Inn building in TID 21

INCREASE:	
TID 21 Fund – Land	$3,186,590
(Acct. No. 421660-621100)	
TID 21 Fund – Debt Proceeds	$3,186,590
(Acct. No. 421-491000)	

Training expenses for the Marina Manager

INCREASE:	
Marina Fund – Harbor Center Marina – Employee Development (Acct. No. 231354-536125)	$5,000
Marina Fund – Harbor Center Marina - Interfund Transfer In (Acct. No. 231-492000)	$5,000
General Fund – Finance - Interfund Transfer Out (Acct. No. 101150-811100)	$5,000
DECREASE:	
General Fund – Finance – Employee Development (Acct. No. 101150-536125)	$5,000

Contract for Department of Public Works Interim Director

INCREASE:	
General Fund – Public Works Admin – Contracted Services (Acct. No. 101310-531100)	$48,000
DECREASE:	
General Fund – City Administration – Contingency (Acct. No. 101141-810101)	$48,000

Correction of account description in Resolution 44-24-25 transferring the salary budget with the movement of the finance functions of Mead Public Library to the Finance Department

INCREASE:	
General Fund – Finance – Part Time Salaries (Acct. No. 101150-510130)	$23,212
DECREASE:	
General Fund – Finance – Overtime (Acct. No. 101150-510111)	$23,212

Purchase of Salt Brine Storage Tank and Skid Mounted Brine Applicator for the reduction of salt usage for winter storms

INCREASE:	
Capital Fund – Property Tax Levy	$48,000
(Acct. No. 400-411100)	
Capital Fund – Public Works – Other Equipment	$48,000
(Acct. No. 400300-659100)	
DECREASE:	
General Fund – Property Tax Levy	$48,000
(Acct. No. 101-411100)	
General Fund – Street Maintenance – Winter Road Supplies	$35,000
(Acct. No. 101331-540250)	
General Fund – Street Maintenance – Contracted Services	$13,000
(Acct. No. 101331-531100)	

Transfer of funds for purchase of KIA Hybrid SUV for utilization at City Hall in trade for Pickup Truck to be utilized at Wastewater

INCREASE:	
Capital Fund – General Government – Vehicles	$41,355
(Acct. No. 400100-651100)	
Capital Fund – Interfund Transfers In	$41,355
(Acct. No. 400-492000)	
Wastewater System Fund – Interfund Transfers Out	$41,355
(Acct. No. 630361-811100)	
DECREASE:	
Wastewater System Fund – Wastewater – Vehicles	$41,355
(Acct. No. 630361-651100)	

Contracts for ash tree treatment, educational post cards regarding tree program and dead tree removal reimbursable through the Urban Forestry DNR Grant

INCREASE:	
Capital Fund – Public Works – Trees/Forestry	$25,000
(Acct. No. 400300-641150)	
Capital Fund – Local Grants	$25,000
(Acct. No. 400-437005)	

Contract for the Maywood and Evergreen Parks Water Quality Improvement Project funded by a grant through Lakeshore Natural Resource Partnership (LNRP)

INCREASE:	
General Fund – Parks – Contracted Services (Acct. No. 101520-531100)	$70,000
General Fund – Local Grants (Acct. No. 101-437005)	$70,000

PASSED AND ADOPTED BY THE CITY OF SHEBOYGAN COMMON COUNCIL _____.

Presiding Officer

_____
Ryan Sorenson, Mayor, City of Sheboygan

Attest

_____
Meredith DeBruin, City Clerk, City of Sheboygan

Ox-Bo Marine
Phone: 9203860175
N5350 Club Grounds Rd
Juneau, WI
Email: boats@oxbomarine.com

2023 SeaArk Work Horse 2472 CUB Jon Boat

Stock#: SHEBOYGAN | VIN#: SOM48120H223 | Year: 2023
Manufacturer: SeaArk | Color: GRAY
URL: https://oxbomarine.com/2023-seaark-work-horse-2472-cub-jon-boat-ozCo.html

Price	$49,995.00
Sales Price	$44,995.00

Description

2023 SeaArk 2472 WORK HORSE CUB

The CUB and Workhorse models are beefed up, square nosed designs of our modified V models. Both models come standard with a 3 degree all-welded hull, standard paint, double-channeled transom, double-welded chine, heavy-duty rub rail, two breaks in side for added strength, eight kilgores with ice runners, an extra rib, bow deck with storage, rear bench seat with storage, and floored area for battery and fuel tank.

Features may include:

3 Degree All-Welded Hull
Standard Paint
Double-Channeled Transom
Double-Welded Chine
Heavy-Duty Rub Rail
Two (2) Brakes in Side
Two (2) Extra Kilgores
Ice Runners on all Kilgores
Extra Rib
Bow Deck w/Storage
Rear Bench Seat w/ Storage
Floored Area for Battery
Push Knees

Factory Installed Features: Flat Top Center Console, .125 Treadplate Aluminum Floor, 33 Gallon Built-in Fuel Tank and Storage Combo, Raised Aft Lid.

Dealer Installed Features: Suzuki 140hp EFI 4-Stroke with Power Tilt and Trim, Multifunction Digital Gauge with Mechanical Controls, Fuel/Water Filter Assembly, Commercial Grade and Salt Water Ready Electrical System with 8 Position Switch Panel with Circuit Breakers, 25A Main Circuit Breaker, Heavy Duty Dual Battery System with Main Power

Battery Switch, Power Point & USB Accessory Outlets, Horn, 2200 GPH Commercial Grade Bilge Pump with Auto Float, LED Navigation Lights, Dometic Hydraulic Steering with Sport Tilt Helm and Stainless Steel Steering Wheel.

2023 Marine Master Tandem Axle Galvanized Trailer with Disc Brakes, LED Lights, Extra Long Side Guides, Boat Buckles, Spare Tire and Transom Saver.

Length: 24'
Beam: 95"
Bottom Width: 72"
Weight Capacity: 2700#
Persons Capacity: 13/1855#
Transom Height: 25"
Hull Gauge: .125 All Welded

Other Custom Options Available:
Safety Grab Rails
Outboard Protection Bar
Bucket Hooks to Sling the Boat
Hand Winch System
Salt Water Package
Light Bar with or without Lights
Grab Handles
Captains Seating
Passenger Seating
Storage Boxes
Dive Platform
Stoaks Box for Stretcher
Flotation Pods with Ladder

Have a CUSTOM need? Ask!

City of Sheboygan
FIRE DEPARTMENT
1326 North 25th Street
SHEBOYGAN, WISCONSIN 53081
(920) 459-3327 OFFICE
(920) 459-0209 FAX

August 23, 2024

Kaitlyn Krueger
828 Center Ave; Suite 110
Sheboygan, WI 53081

Director Krueger,

I am requesting a budget amendment of $35,769.57 for an unanticipated repair for one of our front-line fire suppression vehicles.

On April 16, 2024, Rescue Engine 1862 (a 2010 Pierce Rescue/Pumper), had to be taken out of service and sent in for an unanticipated pump issue. During the routine pump inspection/maintenance, North Star Emergency Services found metal shavings in the pump oil. These shavings were significant enough that they felt it was important to take the unit out of service before permanent damage is done.
The unit was taken to Red Power Diesel (a Pierce Manufacturing Authorized Dealer) to remove the pump from the apparatus for further inspection. They found that a bearing shaft had broken and would have to be replaced. The pump was sent back to the manufacturer and rebuilt and then returned to Red Power for installation.

Red Power also found the foam pump needed repair, and that was sent out for a rebuild as well.

After both units were reinstalled, the vehicle was tested and then returned to the Fire Department.
The total cost of $35,769.57 includes the pump removals, repairs, reinstallation, miscellaneous parts, and labor.

Attached to this letter is the invoice received from Fire Apparatus and Equipment, Inc (Red Power Diesel is an affiliate of theirs), for your reference.

I appreciate the time and assistance you have provided me and the department. If you need anything else, please let me know.

Sincerely,

Eric Montellano
Fire Chief

FIRE APPARATUS AND EQUIPMENT, INC.
5793 W Grande Market Dr., Suite C
Appleton, WI 54913 US
+1 9205743410

BILL TO
Sheboygan Fire Dept.
City Purchasing Department
828 Center Ave. - Suite 208
Sheboygan, WI 53081

SHIP TO
Sheboygan Fire Dept.
Sheboygan Dept. of Public Works
2026 New Jersey Ave.
Sheboygan, WI 53081

INVOICE 25930

DATE 06/19/2024 **TERMS** Net 15

DUE DATE 07/04/2024

P.O. NUMBER
23446

PRODUCT/SERVICE	QTY	RATE	AMOUNT
4P1CJ01A9AA011289			
Mileage ON VEHICLE 57,055 Miles	1	0.00	0.00
ISSUE BEARING PIECES IN OIL	1	0.00	0.00
REFURB PUC	1	24,554.49	24,554.49
Freight Shipping Charge	1	380.64	380.64
PUMP, HYDRAULIC, GEAR, REXROTH	1	1,404.25	1,404.25
-8 AIR BRAKE QUICK FITTING	1	43.21	43.21
SLEEVE 1/2	1	4.25	4.25
3152X12 Brass pipe plug, 3/4"	1	4.25	4.25
PLUG 1/4 3152X4	1	4.25	4.25
NYLON TUBING,1/2OD,FT.	3	1.8366667	5.51
FTG,90SW,06MNPTF,06MNPTF,ST AEROQUIP 2251-6-6S	1	42.71	42.71
3/8-16 X1-1/2	32	0.75	24.00
Lock Washer Alloy Steel 3/8"	32	0.1334375	4.27
O-RING-238 BUNA 70	1	4.25	4.25
Tuff-Torq® Hex Cap Screw Grade 8 Alloy Steel 1/4-20 x 1"	6	0.7083333	4.25
Tru-Torq® USS Flat Washer Thru-Hardened Steel 1/4"	14	0.3035714	4.25
Lock Washer Alloy Steel 1/4"	1	4.25	4.25
Tuff-Torq® Hex Nut Grade 8 Alloy Steel 1/4-20	5	0.85	4.25
DIESEL FUEL; GALLON	15	6.15	92.25
FILTER, PUC HYDRAULIC	2	75.515	151.03
PUC TRANS/DRIVE OIL	16	25.275	404.40

562 110 - 1862 - 7N

Fire Apparatus & Equipment thanks you for your business!

PRODUCT/SERVICE	QTY	RATE	AMOUNT
Labor 2023 WITH PUMP TRANS FULL OF OIL, SPUN OVER AND GOT NO OIL OUT OF GEAR LUBE PUMP ON BACK OF PUMP. REMOVED LUBE LINE FROM TOP OF PUMP AND FOUND IT WAS DRY. UNBOLTED DISCHARGE PIPING FROM TRUCK AND PULLED OFF OF STUDS. UNBOLTED SUCTION PIPING FROM TRUCK. REMOVED COOLING HOSES FROM PUMP. REMOVED LUBE LINES FROM PUMP AND MARKED LINES. UNBOLTED MOUNTING BOLTS AND USED FORKLIFT TO REMOVE FROM TRUCK. BROUGHT INSIDE AND REMOVED COOLING PASSAGES AND IMPELLER FROM TRUCK. FOUND LOTS OF CRACKS AND CHUNKS MISSING FROM THE IMPELLER ASSEMBLY. REMOVED VOLUTE HOUSING FROM PUMP. TESTED OPERATION OF LUBE PUMP. REMOVED OIL PUMP FROM TRUCK. REMOVED BOTTOM PAN OF PUMP TRANS AND FOUND MORE BEARING DEBRIS IN PAN. LIFTED PUMP UP AND STRAPPED ACROSS INTAKES AND USED CHAINFALL TO HOLD UP FRONT. REMOVED STUDS FROM INTAKE AND DISCHARGE FLANGED. INSTALLED NEW ORINGS ON PUMP AND SET NEW PUMP INTO TRUCK. INSTALLED LOWER MOUNTING BOLTS AND BOLTED UP INTAKE TO PUMP HOUSING. INSTALLED COOLANT FITTINGS ON TOP AND BOTTOM AND HOOKED UP HOSES. INSTALLED DISCHARGES AND BOLTED TO PUMP. USED 2 GALLONS OF PUC OIL AND TRANSFER PUMP TO FLUSH OUT OIL SYSTEM. HOOKED UP OIL LINES ONTO PUMP. HOOKED UP MASTER DRAIN LINE WITH NEW FITTING AND PRIMER LINE TO TOP OF PUMP. HOOKED UP OIL LUBE LINES AND INSTALLED FOAM PUMP ON FRONT OF PUMP. HOOKED UP HYDRAULIC LINES TO FOAM PUMP. TOPPED OFF COOLANT ON TRUCK. FILLED PUMP TRANS WITH OIL, INSTALLED PUMP TRANS FILTER, AND INSTALLED DRIVESHAFT USING LOCKTIGHT ON ALL BOLTS. INSTALLED DRIVESHAFT COVER. BROUGHT TRUCK BACK FOR PUMP TEST. MADE IT THROUGH THE FIRST 2 TEST FINE. STARTED TO OVERHEAT. SHUT DOWN TRUCK. HOSE BLEW ONCE TRUCK WAS SHUT DOWN. TILTED CAB AND FOUND PUMP COOLER HOSE GOING INTO LOWER RAD HOSE HAD BLOWN. CALLED PAT AND TALKED OVER ISSUES WITH HIM. REPLACED BLOWN HOSE. PRESSURE TESTED COOLING SYSTEM. PUMP TESTED AND VAC TESTED, BOTH PASSED. RAN FOAM SYSTEM, IT IS WORKING, NO HYDRAULIC LEAKS. ROAD TESTED TRUCK. TOPPED OFF COOLING SYSTEM. CHANGED PUC OIL AND FILTER. ADDED FUEL TO TRUCK.	50	135.00	6,750.00
ISSUE ENGINE OVERHEATING AND COOLANT LEAK	1	0.00	0.00
103F COUPLING 1/2 3300X8	1	4.25	4.25
FITTING 5/8 X 1/2 Hose Barb X Male Pipe	2	3.05	6.10
12-22mm Hose Clamp	2	2.95	5.90
THERMOSTAT - 5273379	1	97.60	97.60
HEATER HOSE,1"ID,FT.	10	11.375	113.75
705-1501 CONSTANT TORQUE CLAMP	1	9.21	9.21
Labor 2023 REPLACED BLOWN HOSE, REPLACED THERMOSTAT, SOME PITTING ON SURFACES SO USED RIGHT STUFF TO SEAL IT. PRESSURE TESTED AND WAS FINE, MADE IT THOUGH PUMP TEST	10	135.00	1,350.00
Misc hardware & shop supply misc. hardware & shop supply	1	292.00	292.00

THANK YOU-----FAE

TOTAL DUE	$35,769.57

Fire Apparatus & Equipment thanks you for your business!

CITY OF SHEBOYGAN
RESOLUTION 44-24-25

BY ALDERPERSONS MITCHELL AND PERRELLA.

JULY 15, 2024.

A RESOLUTION authorizing an amendment to the 2024 budget reflecting a table of organization change for the Finance Department and Mead Public Library.

WHEREAS, the Administrative Services Manager for Mead Public Library retired as of December 31, 2023; and

WHEREAS, the Finance Department hired a part-time limited-term employee to fulfill receipting and accounts payable duties to assist the Library due to this vacancy; and

WHEREAS, the Finance Director and Library Director have reviewed the functionality resulting from the reallocation of duties from the Administrative Services Manager role and the addition of the part-time employee; and

WHEREAS, the Finance Director and Library Director believe it is in the best interest of the City to change the limited-term position to a permanent position in the table of organization; and

WHEREAS, the City Administrator and Human Resources Director were consulted and agree with this change.

NOW, THEREFORE, BE IT RESOLVED: That the table of organization be updated to reflect the removal of the Administrative Services Manager position at Mead Public Library and the addition of a part-time Accounting Clerk position in the Finance Department.

BE IT FURTHER RESOLVED: That the Finance Director is hereby authorized amend the 2024 budget via the following transfers to move the costs associated with the part-time clerk from the Mead Public Library budget to the General Fund budget:

INCREASE:	
General Fund – Finance – Part Time Salaries (Acct. No. 101150-510111)	$23,212
General Fund – Finance – FICA (Acct. No. 101150-520310)	$ 1,440
General Fund – Finance – Medicare (Acct. No. 101150-520311)	$ 337

Correct Account Number for Part Time Salaries is 101150-510130

DECREASE:

Mead Library Fund - Library – Full Time Salaries (Acct. No. 255511-510110)	$23,212
Mead Library Fund – Library – FICA (Acct. No. 255511-520310)	$ 1,440
Mead Library Fund – Library – Medicare (Acct. No. 255511-520311)	$ 337

BE IT FURTHER RESOLVED: That the Finance Department will assume the following tasks on behalf of the Library: accounts payable, receipting and financial reporting.

BE IT FURTHER RESOLVED: That the Common Council approval of this Resolution is contingent upon the Mead Public Library Board of Trustees' approval of an appropriate parallel resolution.

PASSED AND ADOPTED BY THE CITY OF SHEBOYGAN COMMON COUNCIL _____.

Presiding Officer

_____
Ryan Sorenson, Mayor, City of Sheboygan

Attest

_____
Meredith DeBruin, City Clerk, City of Sheboygan

CITY OF SHEBOYGAN
PUBLIC WORKS

2026 New Jersey Ave
Sheboygan, WI 53081

MEMO

To: Travis Peterson

From: Joel Kolste

Date: 9-9-24

Re: Winter Operations - Increased Brine Capabilities Proposal

---

Travis,

During the budget review meeting on 8-26-24 with Casey, he mentioned that we should look into expanding / increasing our utilization of brine with the goal of decreasing our road salt usage.

Brine usage the past several winter seasons has averaged between 40,000 – 60,000 gallons per year.

The Department utilizes brine for two purposes;

- Utilized to pre-wet salt at the spinner (point of application)
- Utilized to pre-treat (anti-icing) roadway surfaces prior to a snow event.

Pre-treatment (anti-icing) of the pavement surfaces is done in advance of a predicted snow event. With current brine storage capacities, and application equipment, the Department is typically able to pre-treat the emergency routes (main roadways). If Neighborhood streets are needed to be treated, the brine tanks need to be refilled. This process often requires an additional day in order to make more brine. The Department also does not pre-treat the City parking lots or recreational trails throughout the City.

Currently, the Department has an automated brine maker along with the following storage capacities;

- 2 – 6,0000 gallon brine tanks (12,000 gallon storage capacity)
- 1 – 2,500 gallon calcium chloride tank

In terms of application equipment, the Department has the following equipment to apply brine as an anit-ice process;

- 6 – dump/salt trucks equipped with slide-in V-box salters with liquid capacity of 800 gallons. Each of these trucks have a spray bar to apply direct application onto pavement. (all salting trucks have liquid for pre-wet but not all have spray bars)

For the Department to pre-treat (anti-ice) the entire City's street network of 200 miles of streets, it is estimated to required 18,000 gallons of brine per event / application.

This cost proposal is being submitted to increase the capaciites and capabilities of the Department's use of brine as a pre-treatment (anti-icing) and pre-wet material with the goal of utilizing less road salt. This proposal adds to existing equipment that has been previously invested.

The proposal includes doubling the current brine storage capacity and additional application equipment to increase efficiencies including equipment to effectively utilize brine in non-traditional areas such as parking lots and recreational trails.

The utilization of salt brine instead of rock salt has several advantages, particularly for communities near rivers and large bodies of water including:

1. **Reduced Environmental Impact**: Salt brine contains only 23% rock salt, requiring less overall salt to cover the same area as rock salt alone. This reduction limits salt runoff into nearby water bodies, helping protect aquatic ecosystems.

2. **Improved Ice Melting Efficiency**: Applied before a snowstorm, salt brine prevents ice from bonding to pavement, making snow and ice removal easier and enhancing road and walkway safety.

3. **Cost-Effectiveness**: Since brine requires less salt, it can be more economical over time. It reduces the frequency of applications and the total amount of salt needed.

4. **Enhanced Coverage**: Brine spreads more evenly across surfaces, ensuring consistent coverage and reducing the risk of untreated, slippery patches.

5. **Reduced Corrosion**: Salt brine is less corrosive than rock salt, which helps extend the life of roads, bridges, and vehicles.

Cost Proposal

STORAGE CAPACITY

Items requested with 2024 Budget Amendment:	Estimated Cost
▪ 2 – 6,250 Gallon Storage Tanks	$15,000
▪ Additional Valves / Piping	$ 8,000
▪ Total	**$23,000**

APPLICATION EQUIPMENT

In the proposed CIP, there are two Tri-Axle Dump Trucks to be replaced in 2025. These trucks will be outfitted with plows, wings, and V-Box salters. One of these trucks is proposed to be retrofitted with an existing V-Box salter which utilizes a smaller brine tank. (400 gallons) The new units will have larger capacity tanks of 800 gallons.

In order to increase brine application efficiencies, we would proposed that each proposed truck be outfitted with new V-Box salters (at the time of purchase) so in order to increase the brine tank capacity of each truck.

The existing V-Box salter would then be kept, and retrofitted into an existing truck that is currently outfitted with only a tailgate spreader and a small add-on brine tank. This change would greatly increase our brine application capabilities. It should be noted that the Department still operates 8 tail-gate spreaders w/100 gallon liquid tanks. This equipment is antiquainted and not condusive to liquid applications. It is the plan of the Department to replace these units with V-Box units as the trucks are replaced through the CIP plan.

Item included in 2025 CIP:

▪ 1 – New V-Box Salter with 800 gallon brine capacity	$90,000
(difference between new install vs. retrofit of existing)	

Currently, the Department does not pre-treat City parking lots and recreational trails. These areas are address with salt only. To reduce salt usage in these areas, we would propose purchasing a 500 gallon tank / sprayer unit that would slide into an existing 1-Ton truck.

Item Requested in 2024 Budget Amendment:

1 – Skid mounted 500 gallon tank / sprayer	$25,000
▪ Total	**$115,000**

	_____
Cost Proposal Total	**$138,000**

Printed: 8/27/2024 9:28:03 AM

Store: 1

Contree Sprayer & Equipment Company, LLC
W9898 Jackson Rd.
Beaver Dam, WI 53916
Tel. (920) 356-0121 Fax (920) 356-0228

Sales Order #67002

Ordered: 8/27/2024
Associate: Dave

Bill To: City of Sheboygan
City of Sheboygan
2026 New Jersey Ave
Sheboygan, WI 53083
920-917-0424

Order Status: Open

INSTRUCTIONS: in stock in beaver dam
102" wide x 194" tall

Qty	Description 1	Description 2	Bin #	Price	Disc %	Ext Price
2	VT6250-102+*	6250 gallon vertical tank 102" diameter x 194" tall standard w/ 3" fitting 1550 pounds	YARD-W	$6,594.00	30%	$13,188.00
1	Shipping Non Taxable	Shipping Charges for Tax Exempt		$250.00		$250.00

Total Qty Ordered: 3 0 3

Percent Unfilled: 100

Subtotal: $13,438.0
Exempt 0 % Tax: + $0.00
TOTAL: $13,438.0
Deposit Balance: $0.00
Balance Due: $13,438.0

Kolste, Joel

From: Ney, Rick
Sent: Friday, January 5, 2024 1:03 PM
To: Kolste, Joel
Subject: FW: Pickup anti-ice sprayer

FYI

From: Redfearn, Troy <Troy.Redfearn@aebi-schmidt.com>
Sent: Wednesday, December 20, 2023 2:04 PM
To: Ney, Rick <Rick.Ney@sheboyganwi.gov>
Subject: Pickup anti-ice sprayer

Hi Rick,

Please click on link to go into the Boss website. https://uk01.l.antigena.com/l/taMFdJjmOuu0HsN21Rp1_bEKKaYQDLusRulganE7~-URGZ5Crrp7shA9glVIzO_pLeh8eC715HDHDgAr1xVHozXbRK4-ZjPzkolYMIY827IJZMTbssqaYbDA3cFouhywDbultuPKJuG-e2KNEPB0j9uZkbnJWiKAA911UScr3SnEdm

The VSI Legacy 305 is $16,000.00

The VSI Legacy 500 is $20,000.00

Let me know if you have any questions.

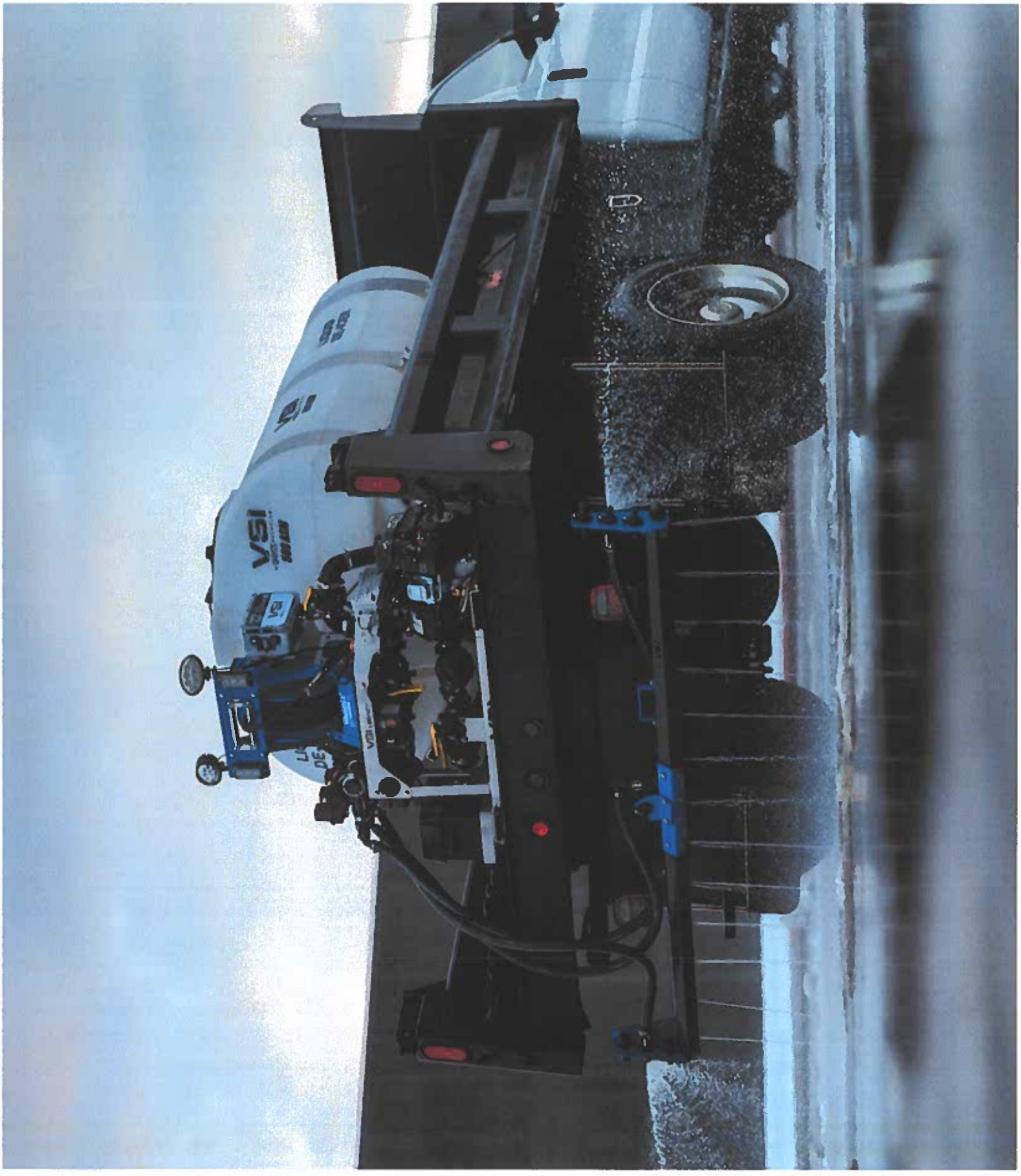
Thanks!

Troy Redfearn
Municipal District/ Outside Sales Manager
Mobile: +1-920-360-4446

Troy.Redfearn@aebi-schmidt.com
Direct Phone:

Monroe Truck Equipment
1151 W Main Ave | DePere, WI 54115 | USA
Phone: +1 920-336-8068 | www.monroetruck.com
Facebook | LinkedIn | Aebi Schmidt Group Blog

"Monroe is now a part of the Aebi Schmidt Group: Same brand and people you know and trust, but now even stronger."


VSI

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

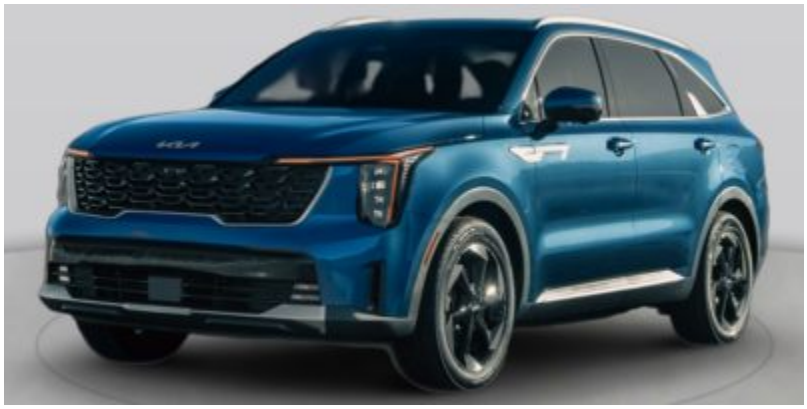
City of Sheboygan

Prepared For: Bernard R Rammer

(920) 459-1342

bernie.rammer@sheboygancounty.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD



Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Quote Worksheet

	MSRP
Base Price	$40,490.00
Dest Charge	$1,375.00
Total Options	$456.00
Subtotal	**$42,321.00**
Subtotal Pre-Tax Adjustments	**$0.00**
Less Customer Discount	($1,136.00)
Subtotal Discount	**($1,136.00)**
Trade-In	$0.00
Subtotal Trade-In	**$0.00**
Taxable Price	**$41,185.00**
Sales Tax	$0.00
Subtotal Taxes	**$0.00**
Subtotal Post-Tax Adjustments	**$0.00**
Total Sales Price	**$41,185.00**

Comments:

2025 Kia Sorento Hybrid Awd in-stock to the specs as detailed. Registration fees are NOT included. Delivery can be made within 10 business days. Subject to final in-stock availability.

Dealer Signature / Date

Customer Signature / Date

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Standard Equipment

Mechanical	
	Engine: 1.6L Turbo GDI 4-Cylinder -inc: idle stop and go
	Transmission: 6-Speed Automatic -inc: paddle shifters, shift-by-wire and drive mode select (comfort, sport, eco, smart, snow)
	Electronic Transfer Case
	Automatic Full-Time All-Wheel
	3.51 Axle Ratio
	60-Amp/Hr 600CCA Maintenance-Free Battery w/Run Down Protection
	Hybrid Electric Motor
	5622# Gvwr
	Gas-Pressurized Shock Absorbers
	Front And Rear Anti-Roll Bars
	Electric Power-Assist Speed-Sensing Steering
	17.7 Gal. Fuel Tank
	Single Stainless Steel Exhaust
	Permanent Locking Hubs
	Strut Front Suspension w/Coil Springs
	Multi-Link Rear Suspension w/Coil Springs
	Regenerative 4-Wheel Disc Brakes w/4-Wheel ABS, Front Vented Discs, Brake Assist, Hill Descent Control, Hill Hold Control and Electric Parking Brake
	Lithium Ion (li-Ion) Traction Battery 1 kWh Capacity
Exterior	
	Wheels: 19" Machine-Finished Aero Alloy -inc: Black and polished chrome
	Tires: 235/55R19
	Steel Spare Wheel
	Compact Spare Tire Stored Underbody w/Crankdown
	Clearcoat Paint
	Body-Colored Front Bumper w/Metal-Look Bumper Insert
	Body-Colored Rear Bumper w/Black Rub Strip/Fascia Accent and Metal-Look Bumper Insert
	Black Bodyside Insert and Black Wheel Well Trim
	Chrome Side Windows Trim and Black Front Windshield Trim

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Exterior	
	Body-Colored Door Handles
	Body-Colored Power Heated Side Mirrors w/Manual Folding and Turn Signal Indicator
	Fixed Rear Window w/Fixed Interval Wiper and Defroster
	Deep Tinted Glass
	Variable Intermittent Wipers
	Fully Galvanized Steel Panels
	Lip Spoiler
	Black Grille w/Chrome Surround
	Smart Power Liftgate Power Liftgate Rear Cargo Access
	Tailgate/Rear Door Lock Included w/Power Door Locks
	Roof Rack Rails Only
	Auto On/Off Projector Beam Led Low/High Beam Daytime Running Auto High-Beam Headlamps w/Delay-Off
	Front Fog Lamps
	Perimeter/Approach Lights
	Headlights-Automatic Highbeams
Entertainment	
	Radio w/Seek-Scan, Clock, Speed Compensated Volume Control, Aux Audio Input Jack, Steering Wheel Controls and Radio Data System
	Radio: AM/FM/SiriusXM Audio System -inc: 12.3" ccNc touchscreen, HD Radio, modem, navigation, over-the-air updates, Kia Connect, Wi-Fi hot spot, 6 speakers, Bluetooth, voice recognition, wireless Apple CarPlay, wireless Android Auto and USB connectivity
	Integrated Roof Antenna
	2 LCD Monitors In The Front
Interior	
	8-Way Driver Seat
	Passenger Seat
	50-50 Folding Bucket Front Facing Manual Reclining Fold Forward Seatback Rear Seat w/Manual Fore/Aft
	Front Center Armrest and Rear Seat Mounted Armrest
	Manual Tilt/Telescoping Steering Column
	Gauges -inc: Speedometer, Odometer, Engine Coolant Temp, Tachometer, Traction Battery Level, Power/Regen, Trip Odometer and Trip Computer
	Power Rear Windows and Fixed 3rd Row Windows

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Interior

	Heated Front Bucket Seats -inc: 10-way power adjustable driver seat w/2-way power lumbar support and 8-way power front passenger seat
	Fixed 50-50 Split-Bench 3rd Row Seat Front, Manual Fold Into Floor, 2 Power and Adjustable Head Restraints
	Leather Steering Wheel
	Front Cupholder
	Rear Cupholder
	Proximity Key For Doors And Push Button Start
	Remote Keyless Entry w/Integrated Key Transmitter, Illuminated Entry and Panic Button
	Remote Releases -Inc: Smart Liftgate Proximity Cargo Access and Power Fuel
	Cruise Control w/Steering Wheel Controls
	Adaptive w/Traffic Stop-Go
	Voice Activated Dual Zone Front Automatic Air Conditioning
	Rear HVAC
	HVAC -inc: Underseat Ducts, Headliner/Pillar Ducts and Console Ducts
	Illuminated Locking Glove Box
	Driver Foot Rest
	Interior Trim -inc: Metal-Look Console Insert and Piano Black/Metal-Look Interior Accents
	Full Cloth Headliner
	SynTex Artificial Leather Seat Trim
	Day-Night Rearview Mirror
	Driver And Passenger Visor Vanity Mirrors w/Driver And Passenger Illumination, Driver And Passenger Auxiliary Mirror
	Full Floor Console w/Covered Storage, Mini Overhead Console w/Storage and 2 12V DC Power Outlets
	Front And Rear Map Lights
	Fade-To-Off Interior Lighting
	Full Carpet Floor Covering
	Carpet Floor Trim
	Trunk/Hatch Auto-Latch
	Cargo Area Concealed Storage
	Cargo Space Lights
	FOB Controls -inc: Cargo Access

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (Complete)

Interior	
	Driver / Passenger And Rear Door Bins
	Power 1st Row Windows w/Driver 1-Touch Up/Down
	Delayed Accessory Power
	Power Door Locks w/Autolock Feature
	Driver Information Center
	Redundant Digital Speedometer
	Trip Computer
	Outside Temp Gauge
	Analog Appearance
	Manual Adjustable Front Head Restraints and Manual Adjustable Rear Head Restraints
	2 Seatback Storage Pockets
	Perimeter Alarm
	Immobilizer
	2 12V DC Power Outlets
	Air Filtration
Safety-Mechanical	
	Highway Driving Assist (HDA)
	Electronic Stability Control (ESC) And Roll Stability Control (RSC)
	ABS And Driveline Traction Control
Safety-Exterior	
	Side Impact Beams
Safety-Interior	
	Dual Stage Driver And Passenger Seat-Mounted Side Airbags
	Parking Distance Warning - Forward & Reverse (PDW-F&R) Front And Rear Parking Sensors
	Blind Spot Collision Warning (BCW) w/Parallel Exit Blind Spot
	Forward Collison-Avoidance Assist (FCA-JT: Cyc/Ped/Junction Turning)
	Lane Keep Assist System (LKAS) Lane Keeping Assist
	Lane Keep Assist System (LKAS) Lane Departure Warning
	Collision Mitigation-Front
	Driver Monitoring-Alert

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Safety-Interior	
	Collision Mitigation-Rear
	Tire Specific Low Tire Pressure Warning
	Dual Stage Driver And Passenger Front Airbags
	Curtain 1st And 2nd Row Airbags
	Airbag Occupancy Sensor
	Power Rear Child Safety Locks
	Outboard Front Lap And Shoulder Safety Belts -inc: Rear Center 3 Point, Height Adjusters and Pretensioners
	Driver Knee Airbag
	Back-Up Camera

WARRANTY	
	Basic Years: 5 Basic Miles/km: 60,000 Drivetrain Years: 10 Drivetrain Miles/km: 100,000 Corrosion Years: 5 Corrosion Miles/km: 100,000 Hybrid/Electric Components Years: 10 Hybrid/Electric Components Miles/km: 100,000 Roadside Assistance Years: 5 Roadside Assistance Miles/km: 60,000

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (Complete)

Selected Model and Options

MODEL

CODE	MODEL	MSRP
U4442	2025 Kia Sorento Hybrid EX AWD	$40,490.00

COLORS

CODE	DESCRIPTION
M4B	Mineral Blue

PRIMARY PAINT

CODE	DESCRIPTION	MSRP
M4B	Mineral Blue	$0.00

SEAT TRIM

CODE	DESCRIPTION	MSRP
GYT	Gray, SynTex Artificial Leather Seat Trim	$0.00

ADDITIONAL EQUIPMENT - PACKAGE

CODE	DESCRIPTION	MSRP
010	Option Group 010 -inc: standard equipment	$0.00

PORT INSTALLED OPTIONS

CODE	DESCRIPTION	MSRP
CF	Carpeted Floor Mats	$225.00
CTS	Carpeted Cargo Mat w/Seatback Protection	$115.00

CUSTOM EQUIPMENT

CODE	DESCRIPTION	MSRP
Delivery	Delivery from Oconomowoc to Sheboygan	$116.00
	Options Total	**$456.00**

Ewald Automotive Group
Scott Kussow | 262-567-5555 | skfleet@ewaldauto.com

Vehicle: [Fleet] 2025 Kia Sorento Hybrid (U4442) EX AWD (✔ Complete)

Price Summary

PRICE SUMMARY

		MSRP
	Base Price	$40,490.00
	Total Options	$456.00
	Vehicle Subtotal	$40,946.00
	Destination Charge	$1,375.00
	Grand Total	**$42,321.00**

Maywood and Evergreen Parks Water Quality Improvement Project

Work agreement with City of Sheboygan (City) and the Lakeshore Natural Resource Partnership (LNRP)

June 10th, 2024

Project Description

The City of Sheboygan is seeking assistance in developing and implementing nature-based water quality improvement projects within Maywood Environmental Park and Evergreen Park, which are located along the Pigeon River corridor. The goal of this project is to improve water quality and restore ecological function and value to Maywood and Evergreen Park properties through implementation of green infrastructure and nature-based solutions that help mitigate runoff, reduce erosion, and reduce nutrient inputs to the Pigeon River and downstream Lake Michigan. Long-term benefits will include more resilient habitat and enhanced recreational opportunities within the park properties and healthier downstream waters.

Deliverables

LNRP will assist the City in implementing the design of a green infrastructure project at Maywood and Evergreen Park

- LNRP will manage contractor services including the bid process, budget management, timeline management, and all contracting/invoicing
  - Secure contracting
  - Baseline Data Collection, field assessments
  - Conceptual design and review
  - Preliminary design plans solidified
- LNRP will prepare grant reports as required by the funder and send to the city using the FFLM template
- LNRP will coordinate meetings between the City and the contractor as needed to ensure ease of implementation
- LNRP will facilitate stakeholder engagement around this project as part of the 9 Key Element Outreach for the Pigeon River

Budget

LNRP will invoice the city quarterly starting he final invoice will be sent once the final report is submitted. This will cover the cost of contracted services and LNRP's time for outreach and to manage the project. The total payment from the City to LNRP will total $70,000.

_____ 6/18/24_

Amy Lentz

Director of Projects (LNRP)

_____

Joe Kerlin

Superintendent of Parks and Forestry (City)

CITY OF SHEBOYGAN
RESOLUTION 109-24-25

BY ALDERPERSONS MITCHELL AND PERRELLA.

OCTOBER 21, 2024.

A RESOLUTION approving City of Sheboygan Health Insurance Portability and Accountability Act (HIPAA) Policies.

WHEREAS, staff from the City's Legal Consultant and Administration departments have determined the City of Sheboygan is a covered entity and must comply with the Health Insurance Portability and Accountability Act; and

WHEREAS, the City of Sheboygan provides a comprehensive, self-funded group health plan; and

WHEREAS, the City of Sheboygan provides ambulance services (EMS) and processes billing for Medicare/Medicaid; and

WHEREAS, training is provided to all personnel handling Protected Health Information (PHI).

NOW, THEREFORE, BE IT RESOLVED: The Common Council hereby indicates their support for and approves the attached HIPAA Policies.

PASSED AND ADOPTED BY THE CITY OF SHEBOYGAN COMMON COUNCIL _____.

Presiding Officer	Attest
_____	_____
Ryan Sorenson, Mayor, City of Sheboygan	Meredith DeBruin, City Clerk, City of Sheboygan

CITY OF SHEBOYGAN
HIPAA POLICIES AND PROCEDURES MANUAL

VOLUME 1:
ADMINISTRATION OF HIPAA COMPLIANCE PROGRAM

ADOPTED: _____

TABLE OF CONTENTS[1]

[1] *Exhibits are provided in a separate document.*

I. GLOSSARY OF DEFINED TERMS

The following terms are used throughout the City of Sheboygan's HIPAA Policies and Procedures Manual:

1. Access, with regard to the security of ePHI, means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. Administrative Safeguard means administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of The City of Sheboygan's Workforce in relation to the protection of that information.

3. Availability means the property that data or information is accessible and useable upon demand by an authorized person.

4. Authorization means a written document or form signed by an Individual or an Individual's Personal Representative that authorizes the Covered Entity or Business Associate to Use or Disclose PHI for a purpose not otherwise permitted under the HIPAA Regulations.

5. BAA means a Business Associate Agreement or contract or other arrangement required by 45 C.F.R. § 164.308(b)(3).

6. Breach means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under this Manual or HIPAA's Privacy Rule which compromises the security or privacy of the PHI. A Breach does not include the following:

    a. Any unintentional acquisition, Access, or Use of PHI by the City of Sheboygan Workforce member (or person acting under the authority of the City of Sheboygan), if such acquisition, Access, or Use was made in good faith and within the scope of job duties and does not result in further Use or Disclosure in a manner not permitted under this Manual or the Privacy Rule.

    b. Any inadvertent Disclosure by the City of Sheboygan Workforce member who is authorized by his/her job duties to Access PHI to another authorized the City of Sheboygan Workforce member, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under this Manual or the Privacy Rule.

    c. A Disclosure of PHI where there is a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

7. Breach Notification Rule or the *HIPAA* Breach Notification Rule means the breach notification rules enforced pursuant to HITECH and codified at 45 C.F.R. Part 164, Subpart D, as may be amended from time to time.

8. Business Associate means a person or entity who, on behalf of the City of Sheboygan, but not in the capacity of the City of Sheboygan's Workforce, performs or assists in the performance certain functions or activities involving the creation, receipt, maintenance, or transmission of PHI, or provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services involving Disclosure of PHI.

9. Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

10. Covered Entity means a health plan, Health Care Clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. For purposes of this Manual, the term "Covered Entity" shall mean the components of the City of Sheboygan, as designated in Section III ("Hybrid Entity Designation") of this Manual, and the City of Sheboygan's health plan.

11. Data Aggregation means, with respect to PHI created or received by a Business Associate or Subcontractor in its capacity as the Business Associate of the City of Sheboygan, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity to permit data analyses that relate to the Health Care Operations of the City of Sheboygan.

12. De-identify or De-identification means the process by which PHI is used to create De-identified Data pursuant to 45 C.F.R. § 164.514(b).

13. De-identified Data or De-identified Information or De-identified Health Information means health information that is not Individually Identifiable Health Information because it neither identifies nor provides a reasonable basis to identify an Individual and is created with one of two methods:

    a. A formal determination by a qualified expert pursuant to 45 C.F.R. § 164.514(b); or

    b. The removal of specified Individual identifiers as well as absence of actual knowledge that the remaining information could be used alone or in combination with other information to identify the Individual pursuant to 45 C.F.R. § 164.514(c).

14. Designated Record Set means the group of records maintained by or for The City of Sheboygan, including medical, billing, enrollment, payment, claims adjudication, care or medical management by or for a health plan, and other records used by the City of Sheboygan, in whole or in part, to make decisions about an Individuals.

15. Disclose or Disclosure means the release, transfer, provision of access to, or divulging in any manner of PHI to an organization or individual that is not the Covered Entity maintaining that information.

16. Electronic Protected Information or "E-PHI," or "ePHI" means PHI transmitted or maintained by electronic format or media.

17. Health Care Clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (a) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (b) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

18. Health Care Operations means activities normal to the business of providing healthcare, including the following activities (non-exhaustive):

    a. Quality assessment and improvement activities, including case management and care coordination;

    b. Competency assurance activities, including health care provider performance evaluation, credentialing, and accreditation;

    c. Conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs;

    d. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the City of Sheboygan; and

    e. Business management and general administrative activities of the entity, including but not limited to De-identifying PHI.

19. Health Plan means an individual or group plan that provides, or pays the cost of, medical care, including the following, singly or in combination: a group health plan as defined in the HIPAA Rules; a health insurance issuer, as defined in the HIPAA Rules; Part A or Part B of the Medicare program; the Medicaid program; the Voluntary Prescription Drug Benefit Program under Part D the Medicare Program; an issuer of a Medicare supplemental policy; an issuer of a long-term care policy, excluding a nursing home fixed indemnity policy; an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers; the health care program for uniformed services; the veterans' health care program; the Indian Health Service program under the Indian Health Care Improvement Act; the Federal Employees Health Benefits Program; an approved State child health plan under title XXI of the Social Security Act, providing benefits for child health assistance; the Medicare Advantage program under Part C of Medicare; a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; or any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

20. HHS means the U.S. Department of Health and Human Services.

21. HIPAA means the Health Insurance Portability and Accountability Act of 1996, as amended.

22. HIPAA Rules means the regulations issued pursuant to HIPAA and HITECH, including without limitation, the Privacy Rule, Security Rule, and Breach Notification Rule.

23. HITECH means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, of the American Reinvestment and Recovery Act of 2009 (Pub. L. 111-5), as amended.

24. Individual means the person who is the subject of the PHI. Unless otherwise provided, the City of Sheboygan will treat a Personal Representative as the Individual for purposes of this Manual.

25. Individually Identifiable Health Information means health information (including demographic information collected from an Individual) that is (a) created or received by a health care provider, health plan, employer, or Health Care Clearinghouse; (b) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and (c) identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

26. Integrity means the property that data or information has not been altered or destroyed in an unauthorized manner.

27. Limited Data Set information that may be Individually Identifiable Health Information, and (a) that summarizes the claims history, claims, or type of claims experienced by Individuals; and (b) PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

    a. Names;
    b. Postal address information, other than town or city, state, and zip code;
    c. Telephone numbers;
    d. Fax numbers;
    e. Electronic mail addresses;
    f. Social security numbers;
    g. Medical record numbers;
    h. Health plan beneficiary numbers;
    i. Account numbers;
    j. Certificate/license numbers;
    k. Vehicle identifiers and serial numbers, including license plate numbers;
    l. Device identifiers and serial numbers;
    m. Web Universal Resource Locators (URLs);
    n. Internet Protocol (IP) address numbers;
    o. Biometric identifiers, including finger and voice prints; and
    p. Full face photographic images and any comparable images.

28. OCR means the U.S. Department of Health and Human Services Office for Civil Rights.

29. Organized Health Care Arrangement or OHCA means:

a. A clinically integrated care setting in which Individuals typically receive health care from more than one health care provider;

b. An organized system of health care in which more than one Covered Entity participates and in which the participating Covered Entities:

i. Hold themselves out to the public as participating in a joint arrangement; and

ii. Participate in joint activities that include at least one of the following:

1. Utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf;

2. Quality assessment and improvement activities, in which Treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or

3. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

c. A group health plan and a health insurance issuer with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer that relates to Individuals who are or who have been participants or beneficiaries in such group health plan;

d. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

e. The group health plans described in paragraph (d) of this definition and health insurance issuers with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers that relates to Individuals who are or have been participants or beneficiaries in any of such group health plans.

30. Payment means the activities undertaken by (a) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (b) a health care provider or health plan to obtain or provide reimbursement for the provision of health care if all such activities in (a) and/or (b) above relate to the Individual to whom the health care is provided and include but are not limited to:

a. Determinations of eligibility or coverage (including coordination of benefits or determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;

b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

c. Billing, claims management, collection activities, obtaining payment under a reinsurance contract (including stop-loss), and related health care data processing;

d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

e. Utilization review activities, including precertification and preauthorization, concurrent and retrospective review of services; and

f. Disclosure to consumer reporting agencies any of the PHI listed in 45 C.F.R. § 164.501 relating to collection of premiums or reimbursement.

31. Personal Representative means a person legally authorized to make health care decisions on an Individual's behalf or to act for a deceased Individual or the estate. A legally authorized personal representative may be a parent of a minor child, a guardian appointed under Chapter 54 of the Wisconsin Statutes, a person designated power of attorney for health care under Chapter 155 of the Wisconsin Statutes, or a person designated durable power of attorney under Chapter 244 of the Wisconsin Statutes.

32. Physical Safeguard means physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

33. Privacy Rule or the HIPAA Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information located at 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164, as amended from time to time.

34. Protected Health Information or PHI means Individually Identifiable Health Information, that is created, received, or maintained by the City of Sheboygan, that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual. Some examples of PHI are (non-exhaustive list):

a. Individual demographic information (e.g., address, telephone number, SSN);

b. Information doctors, nurses and other health care providers put in a client's medical record;

c. Health information about an Individual in the City of Sheboygan's computer system; and

d. Billing information about an Individual.

PHI does not include employment records held by the City of Sheboygan in its role as employer, Individually Identifiable Health Information held in records covered by the Family Educational Rights and Privacy Act, as amended, or regarding a person who has been deceased for more than 50 years.

35. Required by Law means a mandate contained in law that compels an entity to make a Use or Disclosure of PHI and that is enforceable in a court of law, including, but not limited to:

a. Valid court orders and court-ordered warrants;

b. Subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;

c. A civil or an authorized investigative demand;

d. Medicare conditions of participation with respect to health care providers participating in the program; and

e. Statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

36. Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

37. Safeguard means the collective applicable Administrative Safeguards, Physical Safeguards, and Technical Safeguards.

38. Sale of PHI means, except as otherwise provided in the HIPAA Rules, a Disclosure of PHI by the City of Sheboygan, if applicable, where the City of Sheboygan directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

39. Secretary means the Secretary of the U.S. Department of Health and Human Services or his/her designee.

40. Security Incident means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

41. Security Rule means the Standards for the Security of Electronic Protected Health Information located at 45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164.

42. Technical Safeguard means the technology and the policy and procedures for an entity's use that protect ePHI and control access to it.

43. Treatment means the provision, coordination, or management of health care and related services that a health care provider renders to an Individual. Treatment includes management of health care with a third party, consultation between providers relating to an Individual, or the referral of an Individual for care or services to another provider. HIPAA permits Disclosure of PHI for purposes of providing Treatment without an Authorization or need for a Business Associate Agreement.

44. Treatment Records means the registration and all other records that are created in the course of providing services to Individuals for mental illness, developmental disabilities, alcoholism, or drug dependence and that are maintained by the City of Sheboygan under Wis. Stat. § 51.42 or § 51.437 and its staff or by treatment facilities. Treatment Records do not include notes or records maintained for personal use by an individual providing treatment services for the City of Sheboygan under Wis. Stat. § 51.42 or § 51.437 or a treatment facility, if the notes or records are not available to others.

45. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued.

46. Use means, with respect to PHI or ePHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

47. User means a person or entity with authorized Access.

48. Workforce means employees, volunteers, trainees, and other persons, including contractors and agents, whose conduct, in the performance of work for the City of Sheboygan or a Business Associate, is under the direct control of the City of Sheboygan or Business Associate, whether or not they are paid by the City of Sheboygan or Business Associate.

49. Workstation means desktop computers, laptops, and any other devices that perform similar functions, including offsite devices that can access ePHI.

All references made in this Policy are to the section in the HIPAA Rules, federal regulations, or Wisconsin Statutes currently in effect and as subsequently updated, amended or revised.

References	45 C.F.R. § 160.103 45 C.F.R. § 164.105 45 C.F.R. § 164.304 45 C.F.R. § 164.402 45 C.F.R. § 164.501 45 C.F.R. § 164.502 Wis. Stat. §§ 51.42, 51.437 Wis. Stat. Ch. 54, 155, 244
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

II. EFFECTIVE DATE AND CHANGES TO HIPAA PRIVACY POLICIES AND PROCEDURES

1. PURPOSE

To ensure that the City of Sheboygan updates its policies and procedures to comply with any changes under the HIPAA Regulations.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in The City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

These HIPAA Privacy Policies and Procedures are effective as of the date listed in the "Effective Date," as listed at the end of each section. The Privacy Officer or his/her designee will ensure that changes are made to these Policies as appropriate to remain in compliance with all applicable laws.

4. PROCEDURE

A. Changes to these HIPAA Privacy Policies and Procedures may occur at any time with approval from the Human Resources Director.

B. The Privacy Officer and his/her designee is responsible for periodically initiating review of these HIPAA Privacy Policies and Procedures and modifying these Policies (an any related forms or documents) to reflect any necessary changes. The Privacy Officer or his/her designee will review these HIPAA Privacy Policies and Procedures at least annually to ensure such Policies are in accordance with HIPAA.

C. The Privacy Officer or his/her designee is responsible for distributing notice of any such changes to the relevant Workforce members.

D. The Privacy Officer or his/her designee will initiate and oversee Workforce training on any such modifications.

E. If a change to these Policies materially affects the City of Sheboygan's Notice of Privacy Practices ("NPP"), the NPP shall be amended to reflect such a change(s), and the City of Sheboygan shall redistribute the revised NPP, as required under the HIPAA Regulations.

III. HYBRID ENTITY DESIGNATION

1. PURPOSE

Certain departments of the City of Sheboygan will be identified as "Health Care Components" for the purpose of designating the City of Sheboygan as a Hybrid Entity pursuant to HIPAA, HITECH, and the HIPAA Rules.

Although the City of Sheboygan is responsible for HIPAA oversight, compliance, and enforcement requirements, as applicable, the HIPAA Rules apply only to the City of Sheboygan's designated health care components. The purpose of this Policy is to define, in accordance with HIPAA, the Health Care Components of the City of Sheboygan.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

Covered Functions means those functions of a Covered Entity in the performance of which makes the entity a health plan, health care provider, or Health Care Clearinghouse.

Covered Transaction means a "standard transaction" as that term is defined in HIPAA, i.e., a transaction that complies with an applicable standard and associated operating rules adopted under 45 C.F.R. Part 162 (e.g., health care claims or equivalent encounter information, payment and remittance advice, coordination of benefits, claim status, enrollment and disenrollment in a health plan, eligibility, health plan premium payments, and referral certification and authorization).

Health Care Component means a component or combination of components of a Hybrid Entity designated by the Hybrid Entity in accordance with the HIPAA Rules.

Hybrid Entity means a single legal entity: (a) that is a "covered entity"; (b) whose business activities include both covered and non-covered functions; and (c) that designates Health Care Components in accordance with the HIPAA Rules.

3. POLICY

As a health care provider that transmits health information in electronic form in connection with the conduct of Covered Transactions, the City of Sheboygan is a "covered entity" subject to the requirements of HIPAA and HITECH. As a "covered entity", the City of Sheboygan conducts business activities that include both Covered Functions and non-Covered Functions. As such, the City of Sheboygan is permitted under HIPAA to comply with the requirements of HIPAA as a Hybrid Entity. The City of Sheboygan must designate the Health Care Components that will be required to comply with HIPAA, HITECH, and the HIPAA Rules.

For clarity, at all times throughout this HIPAA Policies and Procedures Manual, references to "The City of Sheboygan" shall mean the designated Health Care Components of the City of Sheboygan.

4. PROCEDURE

A. Health Care Component Designation.

1. The City of Sheboygan, in consultation with the appropriate senior leaders/administration, will identify the departments, programs, and functions determined to be Health Care Components.

2. The Human Resources Director, Information Technology Director, and City Administrator will, not less than annually, review the activities of the City of Sheboygan to determine whether any modifications to the designated Health Care Components should be made. Such determinations will be based on whether the unit/department reviewed meets the definition of a Health Care Component. The results of the review will be documented by the Privacy Officer.

3. The Human Resources & Labor Relations Director will communicate the results of the review and designation of the Health Care Components to the and Administration.

4. All components of The City of Sheboygan that perform Business Associate functions for Health Care Components shall be designated Health Care Components.

5. Designated Health Care Components include:

   a. The Fire Department;

   b. The Police and Fire Commission;

   c. The Information Technology Department; and

   d. The Human Resources Department.

B. General Safeguard Requirements.

1. The City of Sheboygan's Health Care Components shall not Disclose PHI to any non-Health Care Components if such Disclosure would be prohibited to an entity that is separate from the City of Sheboygan The City of Sheboygan under the Privacy Rule and The City of Sheboygan HIPAA Policies and Procedures Manual.

2. A member of the City of Sheboygan's Workforce that performs duties for both a Health Care Component and a non-Health Care Component of The

City of Sheboygan shall not Use or Disclose PHI created or received in the course of the member's duties for the Health Care Component while performing duties for the non-Health Care Component if such Disclosure would be prohibited by the Privacy Rule or the City of Sheboygan's HIPAA Policies and Procedures Manual to an entity that is separate from the City of Sheboygan.

3. The City of Sheboygan shall only permit the Use and Disclosure of PHI between Health Care Components and non-Health Care Components of The City of Sheboygan to the same extent, and in the same manner, as The City of Sheboygan is permitted to Use or Disclose PHI to individuals and entities that are separate from The City of Sheboygan.

C. Technical Safeguards.

1. The City of Sheboygan shall implement procedures and Technical Safeguards to limit access to the City of Sheboygan's PHI by Workforce members that perform duties for the non-Health Care Components. These procedures and Technical Safeguards shall include, but not be limited to, Access control and validation procedures to limit Access to electronic records containing PHI.

2. Where connectivity exists, the City of Sheboygan shall maintain Technical Safeguards between its Health Care Components and non-Health Care Components such that the non-Health Care Components are unable to access PHI maintained electronically by the Health Care Components.

D. Documentation. For each designation by the City of Sheboygan of a Health Care Component, the City of Sheboygan shall maintain a written or electronic record of such designation for six years from the date of the designation, or the date when such designation was last in effect, whichever is later.

References	45 C.F.R. § 162.103 – Definitions 45 C.F.R. § 164.103 – Definitions 45 C.F.R. § 164.105(a)(2)(ii) – Safeguard Requirements 45 C.F.R. § 165.105 – Organizational Requirements, Responsibilities of Covered Entity Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

IV. HIPAA POLICIES AND PROCEDURES OVERVIEW

1. PURPOSE

HIPAA requires all Covered Entities to have policies and procedures reflecting HIPAA and HITECH privacy, security, and breach notification mandates. The City of Sheboygan, as a Covered Entity, shall develop administrative policies and procedures reflecting the HIPAA and HITECH privacy, security, and breach notification standards.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in The City of Sheboygan's HIPAA Policy and Procedure Manual Glossary.

3. POLICY

This Policy identifies and establishes procedures for the creation, revision, distribution, and archiving of the City of Sheboygan's HIPAA Policies and Procedures Manual to satisfy HIPAA and HITECH privacy, security, and breach notification requirements.

4. PROCEDURE

A. **HIPAA Policies and Procedures Manual.** HIPAA requires Covered Entities to have policies and procedures to ensure compliance with HIPAA and HITECH privacy, security, and breach notification regulations. The City of Sheboygan is a Covered Entity under HIPAA and is therefore responsible for the research, development, implementation, monitoring, and maintenance of the City of Sheboygan's HIPAA Policies and Procedures Manual.

B. **Training.** Training for the City of Sheboygan's Workforce in privacy, security, and breach notification policies and procedures shall be provided to the City of Sheboygan's Workforce as set forth in the City of Sheboygan's Compliance Training and Education Policy and Procedure.

C. **Reviews and Revisions.** The City of Sheboygan's HIPAA Policies and Procedures Manual shall be reviewed at least annually and may be revised at any time in order to comply or enhance compliance with HIPAA and HITECH standards.

D. **Distribution.** Notice to any substantive revisions to the City of Sheboygan's HIPAA Policies and Procedures Manual will be distributed to Workforce members within five business days of the release of such revisions.

E. **Inquiries.** Any inquiry relative to the City of Sheboygan's HIPAA Policies and Procedures Manual should be directed to the Privacy Officer and/or Security Officer, as appropriate.

F. Sanctions for Non-Compliance. Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

G. Third Party Service Providers. The City of Sheboygan may contract with a third party for assistance in complying with the City of Sheboygan's HIPAA Policies and Procedures Manual.

References	45 C.F.R. § 164.501 – Definitions 45 C.F.R. §§ 164.316(a)-(b) – Policies and Procedures and Documentation Requirements Compliance Training and Education Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**October 1 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

V. APPLICABILITY OF MANUAL

1. PURPOSE

To define the applicability of this Manual to the City of Sheboygan.

2. POLICY

This Manual, including all volumes, applies to the City of Sheboygan, facilities owned or controlled by the City of Sheboygan, and all Workforce members, providers, volunteers, contractors, students, temporary healthcare providers, and Business Associates of the City of Sheboygan who provide services on-site in the City of Sheboygan facilities.

3. PROCEDURE

A. Mandatory Compliance. All Workforce members are responsible for compliance with this Manual. All Workforce members are responsible for completing ongoing education on HIPAA and HITECH as directed by the City of Sheboygan's [Privacy Officer].

References	45 C.F.R. § 164.306(a)(4) – Security Standards. General rules 45 C.F.R. § 164.308(a)(1)(ii)(C) – Sanctions Policy 45 C.F.R. § 164.530(b) – Administrative Requirements. Training 45 C.F.R. § 164.530(e)(1) – Administrative Requirements. Sanctions Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

VI. DESIGNATION OF PRIVACY OFFICER AND SECURITY OFFICER

1. PURPOSE

To designate the City of Sheboygan's Privacy Officer and Security Officer and define the job responsibilities of the designated Privacy Officer and Security Officer.

2. POLICY

The City Administrator shall designate the individual(s) to serve as the Privacy officer and Security Officer for the City of Sheboygan, and the City of Sheboygan shall maintain documentation reflecting such appointment. The Privacy Officer and Security office shall have overall responsibility for the development and implementation of the City of Sheboygan's HIPAA compliance program and the City of Sheboygan's HIPAA Policies and Procedures Manual, in addition to the responsibilities outlined herein.

3. PROCEDURE

A. Privacy Officer Responsibilities. Privacy Officer responsibilities include:

1. Policy and Procedure Management.

   a. Maintain current knowledge of applicable federal and state privacy laws.

   b. Execute, manage, develop, implement, and update/revise the City of Sheboygan's HIPAA Policies and Procedures Manual and ensure that the integrity of the HIPAA Policies and Procedures Manual is maintained at all times.

   c. Monitor industry development, best practice, and OCR settlements and guidance related to privacy of PHI and recommend, as appropriate, for consideration by the City of Sheboygan's.

   d. Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the HIPAA privacy compliance program.

   e. Coordinate with the City of Sheboygan's legal counsel, management, and City Administrator to ensure that the City of Sheboygan maintains appropriate privacy forms, notices, and other administrative materials in accordance with the City of Sheboygan's management and legal requirements.

   f. Monitor and evaluate, on no less than an annual basis, the success of the City of Sheboygan's HIPAA privacy compliance program.

g. Report regularly to the City of Sheboygan's City Administrator regarding the status of the privacy policies.

h. Provide Workforce members, Business Associates, Individuals, government agencies, and vendors with information relative to the City of Sheboygan's HIPAA Policies and Procedures Manual.

2. Individual Rights.

a. Oversee the City of Sheboygan's policies for addressing Individual requests to obtain or amend records, restrict the means of communication, and obtain accountings of Disclosures and ensure compliance with the City of Sheboygan's policies and legal requirements regarding such requests.

b. Establish and oversee grievance and appeals processes for denials of requests related to Individual access or amendments.

3. Complaint Management.

a. Act as the point of contact for receiving, documenting, and tracking all complaints concerning privacy policies or procedures.

b. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the City of Sheboygan's HIPAA Policies and Procedures Manual in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.

4. Training.

a. Oversee and direct HIPAA and HITECH training and orientation to all Workforce members – and Business Associates and appropriate third parties as needed – to ensure all understand the City of Sheboygan's requirements and HIPAA Policies and Procedures Manual requirements relating to the Use and Disclosure of PHI.

b. Initiate, facilitate, and promote activities to foster privacy information awareness within the City of Sheboygan.

c. Maintain appropriate documentation of privacy training.

d. Monitor attendance at all privacy policy training sessions and evaluate participants' comprehension of the information provided at training sessions.

5. Compliance.

   a. Participate in the development and implementation of business associate agreements to ensure privacy concerns, requirements, and responsibilities are addressed. Maintain all business associate agreements and respond appropriately if problems arise.

   b. Maintain necessary documentation in compliance with HIPAA.

   c. Coordinate and participate in disciplinary actions related to the failure of Workforce members to comply with the City of Sheboygan's privacy policies and applicable law.

   d. Cooperate with OCR, other legal entities, and organization officials in any compliance reviews or investigations.

   e. Support management in the assigning of passwords and user identification codes for Access to PHI by authorized users.

   f. Perform periodic privacy risk assessments and ongoing compliance monitoring activities at each of the City of Sheboygan's facilities/locations.

   g. Act as point of contact for the City of Sheboygan's legal counsel in an ongoing manner and in the event of a reported violation.

6. Delegation of Responsibilities. The Privacy Officer may delegate certain job functions to be performed by other qualified individuals. However, the ultimate responsible for the City of Sheboygan's Privacy Rule and Breach Notification Rule compliance remains with the Privacy Officer.

B. Security Officer Responsibilities. Security Officer responsibilities include:

1. Policy and Procedure Management.

   a. Maintain current knowledge of applicable federal and state privacy laws.

   b. Maintain a current and appropriate body of knowledge necessary to perform the City of Sheboygan's information security management function.

   c. Monitor industry development, best practice, and OCR settlements and guidance related to security of PHI and recommend, as appropriate, for consideration by the City of Sheboygan.

   d. Maintain current knowledge of applicable federal and state privacy laws and accreditation standards and monitor advancements in

information security technologies for ensuring organizational adaptation and compliance.

e. Execute, manage, develop, implement, and update/revise the City of Sheboygan's HIPAA Policies and Procedures Manual and ensure that the integrity of the HIPAA Policies and Procedures Manual is maintained at all times.

f. Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the HIPAA security compliance program.

g. Monitor and evaluate, on no less than an annual basis, the success of the City of Sheboygan's HIPAA security compliance program.

h. Report regularly to the City of Sheboygan's City Administrator regarding the status of the security policies.

i. Provide Workforce members, Business Associates, Individuals, government agencies, and vendors with information relative to the City of Sheboygan's HIPAA Policies and Procedures Manual.

2. Oversight and Coordination.

a. Manage and oversee the information security of the City of Sheboygan's ePHI.

b. Monitor information security program compliance and effectiveness in coordination with other compliance and operational assessment functions of the City of Sheboygan.

c. Serve as a member of or liaison to the City of Sheboygan's HIPAA privacy taskforce and information security liaison for users of clinical and administrative systems.

d. Serve as information security consultant to the City of Sheboygan.

e. Cooperate with OCR, other legal entities, and organization officials in any compliance reviews or investigations.

3. Security Management.

a. Establish with management and operations a mechanism to track Access to PHI, within the scope of the City of Sheboygan and as Required by Law, and to allow qualified individuals to review or receive a report on such activity.

b. Review all systems-related information security plans throughout the City of Sheboygan's network to ensure alignment between security and privacy practices and act as a liaison to the information systems department.

c. Certify that IT systems meet predetermined security requirements.

d. Strive to maintain high system availability.

e. Make recommendations for the improvement of operational and procedural changes.

4. Training. Oversee and direct security training and orientation to all Workforce members – and Business Associates and appropriate third parties as needed – to ensure all understand the City of Sheboygan's requirements and HIPAA Policies and Procedures Manual relating to the Use and Disclosure of PHI.

5. Compliance.

a. As requested, participate in assessment of sanctions related to Workforce members' failure to comply with security policies, in cooperation with the Human Resources Department, the Privacy Officer, administration, and legal counsel, as applicable.

b. Initiate, facilitate, and promote activities to encourage information security awareness within the organization and related entities.

c. Conduct investigations of information security violations and work in coordination with management and external law enforcement to resolve these instances.

d. Review instances of noncompliance and work effectively and tactfully to correct deficiencies.

6. Delegation of Responsibilities. The Security Officer may delegate certain job functions to be performed by other qualified individuals. However, the ultimate responsible for the City of Sheboygan's Security Rule compliance remains with the Security Officer.

C. Designation of Privacy Officer and Security Officer.

1. Privacy Officer.

Name of Privacy Officer: Kelly Hendee
Email Address: Kelly.Hendee@sheboyganwi.gov
Phone Number: 920-459-3374

2. Security Officer.

Name of Security Officer: Matt Greenwood
Email Address: matt.greenwood@sheboyganwi.gov
Phone Number: 920-459-3351

References	45 C.F.R. § 164.308(a)(2) – Assigned Security Responsibility 45 C.F.R. § 164.530(a)(1) – Personnel Designations
Attachments	Privacy Officer Job Description and Security Officer Job Description
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

VII. COMPLIANCE TRAINING AND EDUCATION

1. PURPOSE

To help ensure that all relevant members of the City of Sheboygan's Workforce are trained on HIPAA, HITECH, and these HIPAA Privacy Policies and Procedure, and agree to abide by them in order to protect PHI from inappropriate Use and Disclosure.

2. POLICY

Relevant City of Sheboygan Workforce members will be required to complete training regarding the City of Sheboygan's HIPAA and HITECH compliance program within 30 days after commencing work and annually thereafter. The City of Sheboygan will also provide supplemental informal and/or formal training opportunities throughout the year, as appropriate in response to changes in the City of Sheboygan's HIPAA Policies and Procedures Manual, changes in the City of Sheboygan's security safeguarding measures or information technology resources, and in response to changes in industry standards or OCR settlements/guidance.

3. PROCEDURE

A. **Training.** The City of Sheboygan will provide or arrange for the provision of training to all Workforce members on the City of Sheboygan's HIPAA Policies and Procedures Manual with respect to PHI and ePHI as regulated by applicable state and federal law as necessary and appropriate for Workforce members to carry out their work functions. Training shall be provided to all Workforce members who have responsibilities involving Access to, Use, or Disclosure of PHI and other Workforce members deemed necessary within the discretion of the Privacy Officer.

1. Initial Training. Applicable new Workforce members will receive training within 30 days of commencing work with the City of Sheboygan (or within 30 days of commencing a job duty requiring Access to PHI). Training content will include, at a minimum: HIPAA and HITECH overview, state law preemption, privacy and security overview, Use and Disclosure of PHI, minimum necessary standard, permissible Uses and Disclosures of PHI, secure use of the City of Sheboygan's information systems and data, protection from malicious software, password management, Breach and Security Incident response, Breach notification, noncompliance and sanctions, non-retaliation, application of the City of Sheboygan's HIPAA Policies and Procedures Manual to job responsibilities, the identity and location of the City of Sheboygan's Privacy Officer and Security Officer, the requirement that all Workforce members report any potential violations of the City of Sheboygan's HIPAA Policies and Procedures Manual or the HIPAA Rules (whether caused by a Workforce member or service provider) to the Privacy Officer, and other information relative to the protection and security of PHI.

2. Refresher Training. All applicable Workforce members will complete additional training on topics specified by the Privacy Officer and Security Officer at least annually. When formatted as a live training, every effort will be made to offer multiple training sessions at days/times convenient for Workforce members. Sessions will be scheduled until all applicable Workforce members have attended a refresher HIPAA training. When formatted as an online training, Workforce members will be required, upon reviewing the materials, to complete an acknowledgment of training.

3. Additional Training. Additional training or updates, as deemed appropriate by the Privacy Officer and Security Officer, will take place for appropriate Workforce members within a reasonable time period upon the occurrence of:

   a. Revisions to the City of Sheboygan's HIPAA Policies and Procedures Manual;

   b. New information security controls implemented at the City of Sheboygan;

   c. Changes to the City of Sheboygan's information security controls;

   d. Changes in legal or business responsibilities;

   e. New threats or risks to PHI;

   f. Substantial change in federal or state law that affects current functions; or

   g. Identified training need or area of non-compliance.

   Periodic HIPAA reminders are distributed to Workforce members via email and/or ESS (Employee portal.

   Specific HIPAA/HITECH training will take place, as needed, for Workforce members whose job responsibilities require specific knowledge in order to comply with complex laws, regulations, or concepts.

4. Management Responsibility. Workforce members who manage and supervise others are responsible for ensuring that the individuals they supervise attend training, receive information, and understand the City of Sheboygan's HIPAA Policies and Procedures Manual.

5. Scheduling. When formatted as a live training, every effort will be made to offer multiple training sessions at days/times convenient for Workforce members. Sessions will be scheduled until all applicable Workforce members have attended training. All Workforce members are expected to make every effort to attend training sessions.

B. Privacy Awareness and Training Plan.

1. Workforce Training. Each Workforce member who has responsibilities involving the creation, Access to, Use, or Disclosure of PHI will receive training to safeguard PHI and protect the confidentiality and privacy of PHI.

2. Privacy Training Program. The City of Sheboygan has developed, implemented, and regularly reviews a documented program for providing timely and appropriate HIPAA training to Workforce members.

3. Privacy Training Materials. All Workforce members are provided sufficient regular training and supporting reference material to enable them to appropriately identify and protect the confidentiality and privacy of PHI. Such training will include but is not limited to:

    a. An overview of the Privacy Rule relative to the identification and protection of PHI;

    b. A review of all appropriate the City of Sheboygan HIPAA policies, procedures, and standards;

    c. The identity and location of the City of Sheboygan's HIPAA Privacy Officer;

    d. Application of the City of Sheboygan's policies and procedures to job responsibilities;

    e. The requirement that all Workforce members report any potential violations of the City of Sheboygan's policies and procedures or the HIPAA Rules, whether caused by a Workforce member or a service provider, to the Privacy Officer;

    f. Permissible Uses and Disclosures of PHI; and

    g. Other appropriate information relative to the protection of PHI.

C. Security Awareness and Training Plan.

1. Workforce Training. Each Workforce member who has access to the City of Sheboygan's information systems will receive training to protect Confidentiality, Integrity, and Availability of all systems.

2. Security Training Program. The City of Sheboygan has developed, implemented, and regularly reviews a documented program for providing timely and appropriate security training and awareness to Workforce members.

3. Security Training Materials. All Workforce members are provided sufficient regular training and supporting reference materials to enable them to appropriately protect ePHI. Such training will include but is not limited to:

   a. An overview of the Security Rule relative to the Safeguarding of ePHI;

   b. A review of all appropriate the City of Sheboygan HIPAA policies, procedures, and standards;

   c. The identity and location of the City of Sheboygan's Security Officer;

   d. Application of the City of Sheboygan's policies and procedures to job responsibilities;

   e. The requirement that all Workforce members report any potential violations of the City of Sheboygan's policies and procedures or the HIPAA Rules, whether caused by a Workforce member or a service provider, to the Security Officer;

   f. The secure use of the City of Sheboygan's information systems, e.g., log-on procedures (See Log-in Monitoring Policy and Procedure, Password Management Policy and Procedure, and Computer Terminals/Workstations Policy and Procedure);

   g. Significant risks to the City of Sheboygan information systems and data;

   h. The City of Sheboygan's legal and business responsibilities for protecting its information systems and data; and

   i. Security best practices.

4. Protection from Malicious Software. The City of Sheboygan regularly trains and reminds its Workforce members about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data. (See Protection from Malicious Software Policy and Procedure.)

5. Emergency Response. The City of Sheboygan regularly trains its Workforce members about its process for disaster preparedness and emergency response processes. (See Contingency Planning & Recovery Strategy Policy and Procedure.)

6. Password Management. The City of Sheboygan regularly trains and reminds its Workforce members about its process for creating, changing, and safeguarding passwords.

7. Current Training. All Workforce members responsible for implementing Safeguards to protect information systems receive formal training that enables them to stay up to date on current security practices and technology.

8. Security Reminders. The City of Sheboygan will periodically distribute security reminders to all applicable Workforce members. Security reminders will address security topics, including but not limited to: information security policies, information security controls and processes, risks to information systems and ePHI, security best practice, and the City of Sheboygan's information, security, legal, and business responsibilities.

D. Third Party Training. Business Associates are informed about and provided access to the City of Sheboygan's standards as needed. Third parties that Access the City of Sheboygan's information systems or data are informed and are provided access to applicable the City of Sheboygan standards.

E. Policy and Procedure Accessibility. The HIPAA Policies and Procedures Manual is readily available for reference and review by Workforce members.

F. Documentation.

1. Acknowledgement. Each Workforce member attending individualized or small group initial training will be required to sign an Acknowledgement of Initial Training Form. Before being allowed access to PHI, all newly hired Workforce members – and Workforce members new to a position requiring access to PHI – shall be required to provide such Acknowledgement of Initial Training.

   Each Workforce member attending the refresher HIPAA training will be required to sign an Education and Training Attendance Form. The Privacy Officer will maintain a record of attendance at all HIPAA trainings, supplemental/informal education, and reminders for a minimum of six years.

2. Materials. The Privacy Officer will maintain materials presented at each education session (initial, refresher, periodic), whether presented in live or electronic form, for a minimum of six years from the date of its creation or the date when it was last in effect, whichever is later.

References	45 C.F.R. § 164.306(a)(4) – Security Standards. General Rules 45 C.F.R. § 164.308(a)(5)(i)-(ii) – Security Awareness and Training 45 C.F.R. § 164.530(b) – Training 45 C.F.R. § 164.530(j)(1)(i) – Documentation Log-in Monitoring Policy and Procedure Password Management Policy and Procedure Computer Terminals/Workstations Policy and Procedure Contingency Planning & Recovery Strategy Policy and Procedure Protection from Malicious Software Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Acknowledgement of Initial Training Form Education and Training Attendance Form
Responsible Senior Leader	City Administrator
Effective Date	**October 24, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

VIII. SANCTION AND DISCIPLINE POLICY

1. PURPOSE

The City of Sheboygan will ensure that all Workforce members comply with the City of Sheboygan's privacy and security policies and procedures and also applicable provisions of HIPAA, HITECH, and the HIPAA Rules by applying sanction and disciplinary actions appropriate to the breach of policy. This Policy establishes guidelines for such actions.

2. POLICY

Failure to comply with the City of Sheboygan's Policies and Procedures Manual and HIPAA compliance program will result in disciplinary action against the individual committing the violation.

This Policy assists the City of Sheboygan's supervisors and managers of different Workforce members with different discipline processes, sets forth general practices and policies of The City of Sheboygan that should be followed in consultation with the City Administrator, and notifies all Workforce members of consequences for misconduct or violations of The City of Sheboygan's HIPAA Policies and Procedures Manual.

3. PROCEDURE

A. **Sanction/Discipline Policy.** A Workforce member's failure to comply with the City of Sheboygan's HIPAA Policies and Procedures Manual or with the applicable provisions of HIPAA, HITECH, or the HIPAA Rules will be addressed in a timely manner. The City of Sheboygan's HIPAA Policies and Procedures Manual will be enforced consistently across the City of Sheboygan.

B. **Duty to Report.** A Workforce member who fails to report either an actual or suspected violation will have violated the City of Sheboygan's HIPAA Policies and Procedures Manual and may be subject to disciplinary action in accordance with this Policy.

C. **Initial Assessment.** The Privacy Officer is responsible for conducting an initial determination. If complaints or concerns are verified, the complaint/concern may indicate a violation of the City of Sheboygan's HIPAA Policies and Procedures Manual or applicable provisions of HIPAA, HITECH, or the HIPAA Rules.

D. **Sanction/Discipline Procedure.** Complaints against and concerns regarding a Workforce member will be discussed with the individual in question by the Privacy Officer and, if deemed appropriate, will be investigated by the Privacy Officer and City Administrator.

1. Fair and impartial levels of sanctions will be assessed on a case-by-case basis based on the type and magnitude of violation, the specific circumstances of the violation, prior performance reviews and non-compliance, previous education provided, as well as whether the violation

was intentional or non-intentional. Sanctions will be imposed consistently across the City of Sheboygan.

2. Disciplinary action/sanctions may be up to and include termination of employment or of the business relationship, as appropriate. Disciplinary action/sanctions include singularly or in combination (non-exhaustive list):

   a. Attendance and successful completion of additional training;

   b. Verbal reprimand by the individual's immediate supervisor, with summary documentation in the individual's personnel file;

   c. Written warning to the individual's personnel file;

   d. Termination of Access to PHI;

   e. Administrative leave without pay; and

   f. Termination.

3. Final determination of disciplinary action will be as deemed appropriate by City Administrator upon the recommendation of the Privacy Officer and/or Security Officer (as appropriate), presented to the individual and the individual's immediate supervisor (as appropriate), and documented in the personnel file.

4. Notwithstanding this Section D, the Privacy Officer and City Administrator retains discretion to deviate from defined procedures based on the particular facts and circumstances. Each violation will be handled on an individual basis to ensure that disciplinary actions/sanctions are proportional to the severity of the violation.

E. Reporting. The City of Sheboygan shall report sanctions to appropriate regulatory and licensing bodies in compliance with applicable law.

F. Violation of State or Federal Confidentiality Laws and Regulations. Workforce members who knowingly and willfully violate state or federal law for improper Use or Disclosure of an Individual's information may be subject to investigation, prosecution, and/or civil monetary penalties.

G. Documentation. The Privacy Officer will maintain documentation related to compliance enforcement and sanction activities for a minimum of six years from the date of the sanction.

References	45 C.F.R. § 160.316 – Refraining From Intimidating or Retaliatory Acts 45 C.F.R. § 164.308(a)(1)(ii)(C) – Sanction Policy 45 C.F.R. § 164.530(e)(1)-(2) – Sanctions and Documentation 45 C.F.R. § 164.530(j)(2) – Documentation
Attachments	N/A
Responsible Senior Leader	City Administrator

Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

IX. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

1. PURPOSE

The City of Sheboygan is committed to protecting the privacy of Individuals as mandated by applicable federal and state laws and expects its Workforce members to report actual or suspected violations of confidentiality laws without fear of intimidation or retaliation.

2. POLICY

The City of Sheboygan will refrain from threatening, intimidating, coercing, harassing, discriminating against, or taking any other retaliatory action against any Workforce member or other individual for the exercise of any right under, or for participation in any process permitted or required by, HIPAA.

3. PROCEDURE

A. Non-Retaliation for Exercising Rights or Reporting Actual or Suspected Violations. The City of Sheboygan will not retaliate against any Workforce member or other individual for:

1. Exercising any right granted under, or participating in any process established by, applicable state or federal confidentiality laws or regulations, including those rights and processes mandated in HIPAA;

2. Filing a complaint about an improper or unauthorized Use or Disclosure of PHI to the City of Sheboygan Workforce member or with the Secretary;

3. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing related to HIPAA; or

4. Opposing in good faith, any act or practice made unlawful by HIPAA as long as the manner of the opposition is reasonable and does not cause Use or Disclosure of PHI in violation of HIPAA.

B. Open Door Policy. The City of Sheboygan will maintain an "open door policy" at all levels of management to encourage Workforce members to report actual or suspected problems and concerns.

C. Duty to Report. Any Workforce member who observes or becomes aware of or suspects a wrongful Use or Disclosure of PHI is expected to report his/her suspicion, concern, or the wrongful Use or Disclosure of PHI as soon as possible to his/her supervisor, the Privacy Officer, or the Security Officer. A Workforce member who makes a report of suspected or actual improper Use or Disclosure in good faith will not be retaliated against for making the report.

References	45 C.F.R. § 160.316 – Refraining From Intimidation or Retaliation Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

X. RETENTION OF HIPAA DOCUMENTATION

1. PURPOSE

To establish a policy on the retention of the City of Sheboygan's HIPAA compliance-related documents.

2. POLICY

The City of Sheboygan shall maintain all HIPAA required documentation for a period of at least six years from the date of its creation, or the date on which the document was last in effect, whichever is later.

This Policy does *not* apply to the retention of PHI or medical records. Retention of PHI and medical records is governed by The City of Sheboygan's Record Retention follows Municipal Code Section 2-804.

3. PROCEDURE

A. Retention. The City of Sheboygan shall maintain all documents and records created as HIPAA compliance-related documents for a period of at least six years from the date of its creation, or the date on which the document was last in effect, whichever is later.

See the City of Sheboygan's Record Retention Policy which follows Municipal Code Section 2-804 for retention schedules.

B. Compliance Documents. HIPAA compliance-related documents include:

1. Documentation of any action, activity, or assessment performed pursuant to HIPAA or HITECH compliance.

2. Risk assessment and risk management materials created pursuant to the Risk Analysis and Risk Management Policy and Procedure.

3. Documentation that identifies the:

   a. Name, telephone number and address of the City of Sheboygan's HIPAA Privacy Officer and Security Officer;

   b. Name, title, telephone number and address of the individual responsible for receiving complaints;

   c. Name, title, telephone number and address of the individual responsible for obtaining and processing Access, Use, and Disclosure of PHI requests; and

d. Name, title, telephone number and address of the individual responsible for receiving and processing amendment of PHI requests.

4. Methods by which PHI will be De-identified.

5. Sanctions imposed against Workforce members or others who violate the City of Sheboygan's HIPAA Policies and Procedures Manual, HIPAA, HITECH, or the HIPAA Rules.

6. All signed Authorizations and agreed to restrictions.

7. Copies of all Notices of Privacy Practices, including any revisions to such Notices of Privacy Practices.

8. Acknowledgements of the receipt by Individuals of the City of Sheboygan's Notice of Privacy Practices and documentation of any refusals to acknowledge such receipt.

9. Accounting of Disclosure logs.

10. All complaints received and their dispositions.

11. Copies of the City of Sheboygan's HIPAA Policies and Procedures Manual, including all revisions and versions thereof.

Documents may be added or deleted from the above listing as may become necessary by law or as may be established by the City of Sheboygan.

C. Longer Retention. Certain HIPAA documentation may require a record retention period longer than the standard retention period outlined above. These documents include destruction of PHI logs, which shall be maintained permanently.

D. Identifying/Storage of Documents. The Privacy Officer is responsible for identification and storage of records, electronic files, etc. for purposes of complying with this Policy.

References	45 C.F.R. § 164.530(j) – Documentation Record Retention Policy, Employee Handbook Sanction and Discipline Policy and Procedure Risk Analysis and Risk Management Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

XI. DESTRUCTION/DISPOSAL OF PHI

1. PURPOSE

To describe the appropriate methods for disposal and destruction of PHI.

2. POLICY

The City of Sheboygan strives to ensure the privacy and security of all PHI in the maintenance, retention, and eventual destruction/disposal of such information. Destruction/disposal of this information in whatever format shall be carried out as described in this Policy, but always in a manner that leaves no possibility for reconstruction of PHI.

This Policy describes *how* records shall be disposed of/destroyed. *When* records may be disposed of/destroyed is outlined in the City of Sheboygan's Record Retention Policy follows Municipal Code Section 2-804.

PROCEDURE.

A. **Destruction/Disposal Generally.** All destruction/disposal of PHI will be done in accordance with applicable federal and state law and any applicable record retention schedule of the City of Sheboygan. Records containing PHI that have satisfied the period of retention may be destroyed/disposed of by an appropriate method as described in this Policy.

B. **Suspension of Destruction/Disposal.** Records involved in any open investigation, audit, or litigation must not be destroyed/disposed of. If the City of Sheboygan receives notification that any of the above situations have occurred or there is the reasonable potential for such or if the City of Sheboygan anticipates that any of the above situations will occur, the record retention schedule shall be suspended for these records until such time as the situation has been resolved and the continuation of destruction/disposal has been authorized by the City Administrator

If any Workforce member learns of any of the above situations, such Workforce member shall immediately inform the City Administrator, who shall in turn notify the Privacy Officer, Security Officer, corporate counsel, and/or outside counsel as appropriate.

If records have been requested in the course of a judicial or administrative hearing, the Privacy Officer will determine if a qualified protective order should be obtained to ensure that the records are returned to the City of Sheboygan or properly destroyed/disposed of by the requesting party.

C. **Non-Originals.** Records containing PHI that are not originals and that have no retention requirements (e.g., provider copies, shadow charts, etc.) will be destroyed/disposed of by shredding or other comparable method determined by each department. Certification of destruction of non-originals is not required.

D. **Securing Records.** Records containing PHI scheduled for destruction/disposal will be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.

E. **Record of Destruction/Disposal of Originals.** A record of all destruction/disposal of original records/documents containing PHI will be made and retained permanently in accordance with the City of Sheboygan's Retention of HIPAA Documentation Policy and Procedure. Permanent retention is required because the records of destruction/disposal may be needed to demonstrate that the records containing PHI were destroyed/disposed of in the regular course of business. Records of destruction/disposal shall include:

1. Date of destruction/disposal.

2. Method of destruction/disposal.

3. Description of the destroyed/disposed record series or medium.

4. Inclusive dates covered.

5. A statement that the records containing PHI were destroyed/disposed of in the normal course of business.

6. The names, titles, and signatures of the individuals supervising and witnessing the destruction/disposal (when appropriate).

(See Exhibit 1-X Sample Certificate of Destruction.)

F. **Contracted Services.** If destruction/disposal services are contracted, the contract shall:

1. Specify the method of destruction/disposal (which must be consistent with those set forth in this Policy).

2. Specify the time that will elapse between the acquisition and destruction/disposal of data/media.

3. Establish Safeguards against breaches in confidentiality.

4. Provide proof of destruction/disposal.

5. Include a BAA in compliance with the City of Sheboygan's Business Associates and Business Associate Agreement Policy and Procedure.

G. Methods of Destruction/Disposal. PHI will be destroyed/disposed of using a method that ensures the PHI cannot be recovered or reconstructed. Appropriate methods for destruction/disposal are as follows:

Medium	Destruction/Disposal Method
Audiotapes	Methods for destroying/disposing of audiotapes include recycling (tape over) or pulverizing.
Computerized Data/ Computers & Hard Disk Drives (including within some fax machines and copiers)	Methods of destruction/disposal should destroy/dispose of data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy/dispose of the data, but merely deletes the filename from the directory, preventing easy access and making the sector available on the disk so it may be overwritten. Total data destruction/disposal does not occur until the back-up tapes have been overwritten.
Computer Data/Magnetic Media	Methods may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the back-up tapes have been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.
Computer Disks	Methods for destroying/disposing of disks include reformatting, pulverizing, or magnetic degaussing.
Laser Disks	Disks used in "write once-read many" (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing.
Videotapes	Methods for destroying/disposing of videotapes include recycling (tape over) or pulverizing.

H. Additional Information on Disposal of Discarded Paper Containing PHI. On occasion, when copying or faxing documents containing PHI, additional copies are made that are not subject to a retention schedule (because they are copies, not

originals) and that may be disposed of immediately after the purpose for which they were made has been fulfilled. Such paper copies may be disposed of in recycle bins or waste receptacles only as described below:

1. Unsecured recycle bins/waste receptacles should be located only in areas where the public will not be able to access them.

2. When possible, dispose of paper waste containing PHI in receptacles that are secured by locking mechanisms or that are located behind locked doors after regular business hours.

3. Locked recycle bins/waste receptacles must be used to dispose of paper waste containing PHI in unsecure or unattended areas.

4. Paper documents containing PHI may be placed in recycle bins/waste receptacles as described above only if the paper in such bins or receptacles will be disposed of in a manner that leaves no possibility for reconstruction of the information as described in the chart above.

I. Review. The methods of destruction/disposal will be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

J. Device Disposal. Destruction/disposal of devices containing ePHI shall be in accordance with the Device and Media Controls: Disposal Policy and Procedure.

References	45 C.F.R. § 164.310(d)(2)(i) – Device and Media Controls Disposal 45 C.F.R. § 164.530(c) – Safeguards Wis. Stat. § 146.817 – Fetal Tracings Wis. Stat. § 146.819 – Disposition of Records-Cease Practice Wis. Stat. § 895.505 – Disposal of Records Record Retention Policy, Employee Handbook Business Associates and Business Associate Agreement Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Device and Media Controls: Disposal Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Sample Certificate of Destruction
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

XII. BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

1. PURPOSE

To establish a policy and procedure to identify Business Associates and Subcontractors and obtain written assurances from those Business Associates and Subcontractors in order for The City of Sheboygan to document vendor Safeguarding of PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan will enter into BAAs in compliance with the relevant provisions of HIPAA and HITECH to establish permitted and required Uses and Disclosures of PHI. These BAAs must be entered into following the specifications of 45 C.F.R. § 164.504(e).

The City of Sheboygan will allow its Business Associates to create, receive, maintain, and transmit PHI on its behalf if the City of Sheboygan obtains satisfactory written assurances that the Business Associate will appropriately maintain the privacy and security of the PHI and fulfill HIPAA and HITECH Business Associate obligations and any additional privacy, security, and/or breach Safeguarding requirements established by the City of Sheboygan.

4. PROCEDURE

A. Identification of Business Associates. The City of Sheboygan shall ensure that all of the City of Sheboygan's Business Associates have written, valid, executed BAAs in place.

1. BAA Needed. A BAA is needed with all Business Associates. Services include, but are not limited to, claims processing or administration, data analysis, data processing or administration, utilization review, quality assurance, patient safety activities (as defined at 42 C.F.R. § 3.20), billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services. At a minimum, persons or organizations that provide the following types of services involving the creation, receipt, maintenance, transmission, Access to, Use or Disclosure of PHI are considered Business Associates:

    a. Health Care Clearinghouse.

    b. Fundraising or Marketing entity.

    c. Data analysis or Data Aggregation of any kind, including services that De-identify PHI.

d. Professional services, such as consulting, legal, accounting, auditing, actuarial, management or administration, or financial.

e. Accreditation.

f. Electronic data processing, including hardware or software maintenance.

g. Photocopying medical records and other sources of PHI.

h. Document shredding/destruction.

i. Repricing (such as performed by a preferred provider organization to apply negotiated discounts to claims).

j. Storage of PHI (both paper and electronic).

k. Outsourcing services, such as billing or collections.

l. Website hosting.

m. Collection of PHI from Individuals.

n. Vendor of PHI for the City of Sheboygan.

o. Health information exchange organization.

p. Regional health information organization.

q. E-prescribing gateway.

r. Other persons or entities that facilitate data transmission for PHI and that require routine access to PHI.

s. Persons or entities that offer a personal health record to one or more Individuals on behalf of the City of Sheboygan.

In addition, if the City of Sheboygan is conducting business with a vendor that provides data transmission services of PHI and requires access to such information (e.g., health information exchange; regional health information organization, or e-prescribing gateway) or a vendor that allows the City of Sheboygan to offer Workforce members access to a personal health record, that vendor will be treated as a Business Associate.

2. BAA Exceptions. A BAA is not required in the following situations:

a. Disclosure of PHI to a health care provider for Treatment purposes;

b. Disclosures of PHI to an Individual's insurer for Payment purposes;

c. With members of the City of Sheboygan's OHCA(s), as applicable;

d. With members of the City of Sheboygan's Workforce;

e. Private or public courier service;

f. Disclosures of Limited Data Set (however, a Data Use Agreement is required and should be completed in accordance with Section B of this Policy and the Limited Data Sets and Data Use Agreement Policy and Procedure);

g. Disclosures to researchers for Research purposes, provided that appropriate consent has been obtained from Research subjects or a Waiver of Authorization has been obtained from the Institutional Review Board acting as the Privacy Board and consistent with the City of Sheboygan's Uses and Disclosures of PHI for Research Purposes Policy and Procedure, as applicable;

h. Disclosures to financial institutions for the purpose of (i) processing consumer-conducted financial transactions by debit, credit, or other payment, (ii) clearing, checking, initiating, or processing electronic fund transfers, or (iii) conducting any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums.

3. Confidentiality. Contractors that do not require PHI in order to fulfill their contractual responsibilities to the City of Sheboygan are not considered Business Associates. However, because such contractors may encounter PHI incidentally in the process of performing their duties under their contracts, and because the City of Sheboygan has a duty to Safeguard PHI, all of the City of Sheboygan's contracts for services will contain a basic confidentiality clause.

4. Subcontractors. Subcontractors that create, receive, maintain, or transmit PHI on behalf of a Business Associate are also Business Associates. However, the City of Sheboygan is not required to enter into a BAA with a Business Associate that is a Subcontractor. Instead, the City of Sheboygan's Business Associate must obtain satisfactory assurances in the form of a written contract or other arrangement with the Subcontractor.

5. Content of BAAs. The City of Sheboygan's BAAs will include, at a minimum, all terms required in BAAs pursuant to HIPAA and HITECH and the terms outlined in this Policy. The City of Sheboygan reserves the right to add any additional terms to its BAAs as it deems reasonable and appropriate.

6. Verification of Secure Practices. Depending on the potential risks to the security of the City of Sheboygan's PHI as determined by a risk analysis,

the City of Sheboygan may require verification of secure practices by the Business Associate, including the provision of documentation of secure practices and/or documentation of reviews of secure practices by a qualified third party.

B. Data Use Agreement. A Data Use Agreement, and not a BAA, is required with any third party or Business Associate to whom the City of Sheboygan will Disclose a Limited Data Set. See the City of Sheboygan's Limited Data Sets and Data Use Agreements Policy and Procedure for more information on Data Use Agreements.

C. BA Agreements.

1. Disclosure of PHI. No member of the City of Sheboygan's Workforce is permitted to Disclose PHI to a Business Associate or Subcontractor (collectively, "BA") or to allow a BA to Access or obtain PHI on behalf of the City of Sheboygan unless a BAA has been executed between the City of Sheboygan and the BA. The BAA must include provisions that meet the standards listed in this Policy. The BA must sign the BAA prior to performing any services. No Access to PHI will be allowed, no account will be set up, and no money will be paid for products or services until the BAA is signed.

2. Negotiation and Execution of BAAs.

   a. Any BAA that does not follow the City of Sheboygan's template shall be reviewed and approved by The City of Sheboygan's Privacy Officer or his/her designee or the City Administrator before the City of Sheboygan may execute the BAA.

   b. Any BAA that authorizes De-identification, Data Aggregation, or Access to sensitive PHI by a BA must be authorized by the City of Sheboygan's Privacy Officer.

   c. The Privacy Officer and City Administrator are authorized to sign BAAs on behalf of the City of Sheboygan.

3. Contract Renewal. Contract renewal will be monitored for continued HIPAA compliance by the Privacy Officer.

4. Retention. BAAs and any appropriate supporting documentation shall be retained for a period of at least six years after the expiration or termination of the Business Associate relationship, which for purposes of this Policy will include such time after a BAA is terminated but the BA still maintains any PHI due to the infeasibility of return or destruction.

References	45 C.F.R. § 160.103 – Definitions 45 C.F.R. § 164.314(2)(i) – Business Associate Agreement 45 C.F.R. § 164.502(e) – Disclosures to Business Associates 45 C.F.R. § 164.504(e)(2) – Business Associate Agreement 45 C.F.R. § 164.514(e) – Limited Data Set 45 C.F.R. § 164.532 – Permission for Research Limited Data Sets and Data Use Agreements Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Template Business Associate Agreement (For Use When The City of Sheboygan is a Covered Entity) Template Subcontractor Business Associate Agreement (For Use when The City of Sheboygan is a Business Associate with a Downstream Subcontractor)]
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

XIII. LIMITED DATA SETS AND DATA USE AGREEMENTS

1. PURPOSE

To establish a policy and procedure for the Use and Disclosure of Limited Data Sets and use of Data Use Agreements.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in The City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

In accordance with the requirements of the HIPAA Rules, the City of Sheboygan may Use PHI to create a Limited Data Set and may Disclose PHI in the Limited Data Set to a recipient if the recipient and the City of Sheboygan have entered into a Data Use Agreement.

4. PROCEDURE

A. **Using PHI to Create a Limited Data Set.** The City of Sheboygan may Use PHI to create a Limited Data Set, or may Disclose PHI to a Business Associate to create a Limited Data Set, regardless of whether the Limited Data Set is to be Used by the City of Sheboygan or another recipient.

B. **Use of a Limited Data Set.** The City of Sheboygan may Use or Disclose a Limited Data Set to a recipient only for the purposes of Research, public health, or Health Care Operations, and only if the City of Sheboygan enters into a Data Use Agreement with the recipient.

If the City of Sheboygan wishes to Disclose any of the following information (related to an Individual or any relative, employer, or household members of the Individual) to the recipient, a Data Use Agreement cannot be used:

1. Names;
2. Postal address information, other than town or city, state, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;

8. Health plan beneficiary numbers;

9. Account numbers;

10. Certificate/license numbers;

11. Vehicle identifiers and serial numbers, including license plate numbers;

12. Device identifiers and serial numbers;

13. Web Universal Resource Locators (URLs);

14. Internet Protocol (IP) address numbers;

15. Biometric identifiers, including finger and voice prints; or

16. Full face photographic images and any comparable images.

If any of the above elements will be disclosed, a BAA may be necessary. Please see the City of Sheboygan's Business Associates and Business Associate Agreement Policy and Procedure for more information on when a BAA may be necessary.

C. Data Use Agreement Contents.

1. The City of Sheboygan must obtain satisfactory assurances from the intended recipient of the Limited Data Set by entering into a Data Use Agreement prior to the Disclosure of the Limited Data Set to the recipient.

2. The Data Use Agreement must document that the recipient will only Use and Disclose the Limited Data Set for limited purposes.

3. The Data Use Agreement between the City of Sheboygan and the Limited Data Set recipient must be reviewed by Privacy Officer and meet the following requirements:

    a. Be in writing and signed by the City of Sheboygan and the Limited Data Set recipient prior to providing Access to the Limited Data Set;

    b. Establish the permitted Uses and Disclosures of the Limited Data Set by the recipient, which must be consistent with limiting its Use and Disclosure to Research, public health, or Health Care Operations;

    c. May not authorize the recipient to Use or further Disclose the information in any manner that would violate HIPAA or HITECH if done by the City of Sheboygan;

    d. Establish who is permitted to Use or receive the Limited Data Set; and

e. Provide that the recipient will:

i. Not Use or Further Disclose the Limited Data Set other than as permitted by the Data Use Agreement or as otherwise Required by Law;

ii. Use appropriate Safeguards to prevent Use or Disclosure of the Limited Data Set other than as provided for by the Data Use Agreement;

iii. Report to The City of Sheboygan any Use or Disclosure of the Limited Data Set not provided for by the Data Use Agreement of which it becomes aware;

iv. Ensure that any agents to whom the recipient provides the Limited Data Set agree to the same restrictions and conditions that apply to the recipient with respect to the Limited Data Set; and

v. Not identify the Limited Data Set or contact the Individuals.

The City of Sheboygan reserves the right to add any additional terms to its Data Use Agreements as it deems reasonable and appropriate.

In the event The City of Sheboygan learns of a Limited Data Set recipient's pattern of activity or practice that constitutes a material Breach or violation of the Data Use Agreement, the City of Sheboygan will take steps to cure the Breach, end the violation and discontinue Disclosure of PHI to the recipient.

References	45 C.F.R. § 164.514(e) – Limited Data Set 45 C.F.R. § 164.530 – Administrative Requirements Business Associates and Business Associate Agreement Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	n/a
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	**November 1st of even years**
Revisions	

40977226_3.DOCX

CITY OF SHEBOYGAN
HIPAA POLICIES AND PROCEDURES MANUAL

VOLUME 2:
PRIVACY POLICIES AND PROCEDURES

ADOPTED: _____

TABLE OF CONTENTS[1]

[1] *Exhibits are provided in a separate document.*

I. AUTHORIZATION FOR USE AND DISCLOSURE OF PHI

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures for obtaining authorization from Individuals for release of PHI when an authorization is Required By Law. In addition, to define procedures for revocation of authorization by Individuals for access, release, Use, and/or Disclosure of their PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan HIPAA Policies and Procedures Manual Glossary.

3. POLICY

A. **Authorizations.** Except as otherwise permitted or required by the Privacy Rule (*see, e.g.,* City of Sheboygan's Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations Policy and Procedure and Incidental Uses and Disclosures of PHI Policy and Procedure), the City of Sheboygan will not Use or Disclose PHI without a valid authorization. The City of Sheboygan, including any Business Associates on behalf of City of Sheboygan, may choose to obtain a signed authorization in situations where it is not required. Global authorizations may be obtained from the Individual as determined appropriate by the City of Sheboygan. When the City of Sheboygan receives an authorization, the City of Sheboygan will Use and Disclose PHI consistent with such authorization.

B. **Revocation of Authorization.** Individuals have the right to revoke any authorization to Use or Disclose their PHI at any time. Information that has been Disclosed under an authorization cannot be recalled, but revocation of an authorization prevents further Uses or Disclosures under the authorization.

4. PROCEDURE

A. **Authorization Requirements.**

1. The City Administrator or his/her designee will be responsible for ensuring that authorizations are obtained when Use or Disclosure of PHI is necessary.

2. The provision of Treatment, Payment, including eligibility for benefits, and Health Care Operations may not be conditioned upon the Individual's provision of an authorization for the Use or Disclosure of PHI.

3. Each authorization for the Use or Disclosure of an Individual's PHI will be written in easy-to-read language and will include, at a minimum, the following information:

   a. A specific and meaningful description of the information to be Used or Disclosed, including an affirmative note of any sensitive health

information to be disclosed (e.g., alcohol or other drug abuse records, mental health records, sexual assault records, HIV test results);

b. The name or identification of the person or class of person(s) authorized to make the Use or Disclosure;

c. The name or identification of the person or class of person(s) to whom the requested Use or Disclosure may be made;

d. An expiration date, condition, or event that relates to the Individual or the purpose of the Use or Disclosure;

e. A description of each purpose of the requested Use or Disclosure;

f. A statement that the authorization will expire after twelve (12) months unless the Individual has opted for a shorter or longer time (e.g., part of an approved research study or expected to continue to receive services for a longer period of time);

g. A statement of the Individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the Individual may revoke the authorization;

h. A statement that upon the City of Sheboygan's receipt of the written notice of revocation, the City of Sheboygan's further Use or Disclosure of PHI shall cease immediately except to the extent that the City of Sheboygan has acted in reliance upon the authorization or to the extent that Use or Disclosure is otherwise permitted or Required by Law;

i. A statement that the information may only be released with the written authorization of the Individual, except as Required by Law;

j. A statement that the Individual may refuse to sign the authorization;

k. A statement either that: (i) Treatment, Payment, and eligibility for benefits will not be conditioned upon the Individual's provision of an authorization or (ii) the circumstances under which Treatment, Payment, and/or eligibility for benefits will be conditioned upon the Individual's provision of an authorization (e.g., Research, and provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the Disclosure of the PHI to such third party);

l. If applicable (e.g., Sale of PHI), a statement that the Use or Disclosure will result in direct or indirect remuneration for a third party;

m. A statement that a copy of the signed authorization will be provided to the Individual;

n. The signature of the Individual and date signed; and

o. If the authorization is signed by a Personal Representative of an Individual, a description of the representative's authority to act on behalf of the Individual.

4. The City of Sheboygan will attempt to use its Authorization for Use and Disclosure of PHI Form – rather than third party forms – for authorizations as possible.

B. **Revocation Request.**

1. Form of Request. All requests for revocation of an Individual's authorization to access, release, Use or Disclose PHI must be submitted to the Privacy Officer or his/her designee in writing. When possible, the City of Sheboygan will provide its Revocation Form to Individuals. If the City of Sheboygan's Revocation Form is not used, the Privacy Officer will confirm that the revocation is specific enough to permit identification of the authorization that is being revoked. Oral requests will not be honored. The HIPAA Privacy Officer shall be consulted with any questions on specificity of revocation and/or oral requests.

2. Processing Request. Upon receipt of a written revocation – and, if applicable, confirmation of specificity of the request – the Privacy Officer will notify the relevant staff and impacted Business Associates that a revocation has been received and that no further PHI may be released as specified in the authorization.

C. **Documentation.** The City of Sheboygan shall maintain Individuals' authorizations for Use and Disclosure of PHI (including Authorization for Use and Disclosure of PHI Forms) and Individuals' written revocations on the Use and Disclosure of PHI (including Revocation Forms) consistent with the Retention of HIPAA Documentation Policy and Procedure.

D. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.508 – Uses and disclosures for which an authorization is required 45 C.F.R. § 164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required Use and Disclosure to Carry Out Treatment, Payment and Health Care Operations Policy and Procedure Incidental Uses and Disclosures of PHI Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Authorization for Use and Disclosure of PHI Form Revocation Form
Responsible Senior Leader	Privacy Officer

Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

II. USES AND DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS (TPO)

1. PURPOSE

To establish a policy and identify the procedures for Uses or Disclosures of PHI for carrying out Treatment, Payment, and Health Care Operations in accordance with HIPAA.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

Except as permitted or Required by Law, the City of Sheboygan will not Use or Disclose (including obtaining) PHI without Individual authorization for purposes other than Treatment, Payment, or Health Care Operations.

All Workforce members are trained to understand and identify elements of PHI.

4. PROCEDURE

A. **City of Sheboygan's TPO Purposes.** The City of Sheboygan may Use and Disclose PHI without an Individual's authorization for the City of Sheboygan's own Treatment, Payment, or Health Care Operations purposes.

B. **Another Covered Entity's TPO Purposes.** The City of Sheboygan may Disclose PHI without an Individual's authorization as follows:

1. To another Covered Entity for the Treatment of the Individual who is the subject of the PHI.

2. To another Covered Entity for the Payment activities of that entity.

3. To another Covered Entity for the Health Care Operations activities of the entity that receives the information if each entity (both the City of Sheboygan and the other entity) either has or had a relationship with the Individual who is the subject of the PHI, the PHI pertains to such relationship, and the Disclosure is:

    a. For Health Care Operations regarding conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting healthcare providers and patients with information about Treatment alternatives, and related functions that do not include Treatment, reviewing the competence or qualification of healthcare

professionals, evaluating practitioner and provider performance or Health Plan performance, or credentialing activities.

b. For the purpose of healthcare fraud and abuse detection or compliance.

C. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.506 – Uses and disclosure to carry out treatment, payment, or health care operations Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

III. USES AND DISCLOSURES NOT REQUIRING INDIVIDUAL AUTHORIZATION

1. PURPOSE

To establish a policy and identify procedures for how the City of Sheboygan will Use and Disclose PHI without Individual authorization.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan may Use or Disclose PHI without Individual authorization for reasons based on public policy and as permitted or Required by Law.

4. PROCEDURE

A. **Use and Disclosure Without Authorization.** The City of Sheboygan may Use or Disclose PHI without Individual authorization in the following circumstances:

1. Treatment Alternatives. Information about treatment alternatives or other health-related benefits and services that may be of interest to Individuals. However, when the City of Sheboygan is receiving remuneration above the cost of communication for the provision of such information, authorization is required unless such information is provided via face-to-face communication.

2. Family and Friends Involved in Care. Disclosures to family members and those involved in the Individual's care consistent with the City of Sheboygan's Use and Disclosures of PHI to Persons Involved in the Individual's Care and for Notification Purposes Policy and Procedure.

3. Serious Threat to Health or Safety of Self or Others. Consistent with applicable law and standards of ethical conduct, the City of Sheboygan may Use and Disclose PHI to the proper authorities (i.e., person(s) reasonably able to prevent or lessen the threat, including the target of the threat) if the City of Sheboygan believes, in good faith, that such Use or Disclosure is necessary (i) to prevent or lessen a serious and imminent threat to the health or safety of a person (including, but not limited to, the subject Individual) or the public and (ii) for law enforcement authorities to identify or apprehend an Individual (because of a statement by an Individual admitting participation in a violent crime that the City of Sheboygan reasonably believes may have caused serious physical harm to the victim or where it appears from all the circumstances that the Individual has escaped from a correctional institution or from lawful custody).

4. Activities Related to Death. The City of Sheboygan may Disclose PHI to coroners, medical examiners, and funeral directors so they can carry out their duties related to an Individual's death, such as identifying the body, determining cause of death, or in the case of funeral directors to carry out funeral preparations.

5. Public Health Activities. The City of Sheboygan may Use or Disclose PHI for the following public health activities to:

   a. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

   b. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

   c. A person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity;

   d. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the City of Sheboygan or a public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation;

   e. An employer, about an Individual who is a member of the workforce of the employer if:

      i. The City of Sheboygan provides health care to the Individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the Individual has a work-related illness or injury;

      ii. The PHI Disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

      iii. The employer needs such findings in order to comply with its obligations, under the Occupational Safety and Health Administration standards or under state law having a similar

purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

iv. The City of Sheboygan provides written notice to the Individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer.

f. A school, about an Individual who is a student or prospective student of the school if the PHI Disclosed is limited to proof of immunization, the school is required by state or other law to have such proof of immunization prior to admitting the Individual, and the City of Sheboygan obtains and documents the agreement to the Disclosure.

6. Victims of Abuse, Neglect, or Domestic Violence. Except for reports of child abuse or neglect permitted by the public health reporting outlined in Section 4.A.5.b of this Policy and Procedure, the City of Sheboygan may disclose PHI about an Individual whom the City of Sheboygan reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

a. To the extent the Disclosure is Required by Law and the Disclosure complies with and is limited to the relevant requirements of such law;

b. If the Individual agrees to the Disclosure; or

c. To the extent the Disclosure is expressly authorized by statute or regulation and (i) in the exercise of professional judgment, the City of Sheboygan believes the Disclosure is necessary to prevent serious harm to the Individual or other potential victims or (ii) the Individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that PHI for which Disclosure is sought is not intended to be used against the Individual and that an immediate enforcement activity that depends upon the Disclosure would be materially and adversely affected by waiting until the Individual is able to agree to the Disclosure.

The City of Sheboygan will promptly inform the Individual that such a report has been or will be made, except if, in the exercise of professional judgment, it believes informing the Individual would place the Individual at risk of serious harm or the City of Sheboygan would be informing a Personal Representative, and the City of Sheboygan reasonably believes the Personal Representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of

the Individual as determined by the City of Sheboygan, in the exercise of professional judgment.

7. Health Oversight. The City of Sheboygan may Disclose PHI to a health oversight agency for oversight activities authorized by law in compliance with the HIPAA Rules.

8. Judicial and Administrative Proceedings. The City of Sheboygan may Disclose PHI in the course of any judicial or administrative proceeding:

   a. In response to a court order signed by a judge, provided that the City of Sheboygan Discloses only the PHI expressly authorized by such order; or

   b. In response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order signed by a judge in compliance with the HIPAA Rules.

9. Law Enforcement Purposes. The City of Sheboygan may Disclose PHI for a law enforcement purpose to a law enforcement official in compliance with the HIPAA Rules (e.g., victims of a crime, crime on premises, reporting crime in emergencies).

10. Decedents. The City of Sheboygan may Disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

11. Donations. The City of Sheboygan may Disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

12. Research. The City of Sheboygan may Disclose PHI for Research purposes consistent with the HIPAA Rules and the City of Sheboygan's Use and Disclosure of PHI for Research Purposes Policy and Procedure.

13. Workers' Compensation. The City of Sheboygan may Disclose PHI authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

B. **Other Situations When Requirements are Met.** The City of Sheboygan may Use or Disclose PHI without Individual authorization (i) as Required by Law and (ii) for other reasons, when specific requirements are met. The situations in which PHI may be Used or Disclosed include, but are not limited to, situations involving:

1. Order of the court
2. Disclosures to Health Plan sponsor
3. Organ tissue donation

4. Military and veterans
5. Workers' compensation
6. Public health and safety
7. Health oversight activities
8. Lawsuits and disputes
9. Law enforcement
10. National security and intelligence activities; and
11. Inmates

C. **Documentation.** The City of Sheboygan shall record each Use and Disclosure made under this Policy and Procedure on the Accounting of Disclosures Log, consistent with the Accounting of Disclosures of PHI Policy and Procedure and Retention of HIPAA Documentation Policy and Procedure.

D. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.502(g)(5) – Uses and disclosures of protected health information: General Rules, Abuse, neglect, endangerment situations 45 C.F.R. § 164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required Accounting of Disclosures of PHI Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure Uses and Disclosures of PHI to Persons Involved in the Individual's Care and for Notification Purposes Policy and Procedure Uses and Disclosures of PHI for Research Purposes Policy and Procedure
Attachments	N/A
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

IV. PERSONAL REPRESENTATIVES

1. PURPOSE

To establish a policy and identify procedures for how the City of Sheboygan will address (1) Personal Representatives and (2) the privacy rights of minors who are not emancipated from the care of their parents or guardian.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan shall treat a Personal Representative the same as it would treat the Individual who is the subject of the PHI, unless any one of the exceptions applies.

4. PROCEDURE

A. **General Rules**. Unless one of the below exceptions applies, the City of Sheboygan shall treat a Personal Representative as the Individual for purposes of the Privacy Rule.

B. **Access to Records.** Regardless, however, of whether a parent is the Personal Representative of a minor child, the City of Sheboygan is permitted to Disclose to a parent, or provide the parent with access to, a minor child's PHI when and to the extent it is permitted or Required by Law (including relevant case law). The City of Sheboygan shall not Disclose a minor child's PHI to a parent, or provide a parent with access to such PHI, when and to the extent it is prohibited under state or other laws (including relevant case law).

C. **Parents as Personal Representative when State Law is Silent.** If state or other applicable law is silent concerning parental access to minor's PHI, then the City of Sheboygan has discretion to provide or deny a parent with access to the minor's PHI if doing so is consistent with state or other applicable law and provided the decision is made by a licensed healthcare professional in the exercise of professional judgment.

D. **Exceptions to a Parent as a Personal Representative.** There are three circumstances in which the parent is not the Personal Representative with respect to certain PHI about his or her minor child. These exceptions generally track the ability of certain minors to obtain specified healthcare without parental consent under state or other laws or standards of professional practice. In these situations, the parent does not control the minor's health care decisions and, thus, under the Privacy Rule, does not control the PHI related to that care. The three exceptions are as follows:

1. When state or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service and the minor consents to the health care service (e.g., adolescents have the right to consent to certain mental health care treatment without parental consent);

2. When someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent (e.g., court order grants the right to make health care decisions to someone other than a parent); and

3. When a parent agrees to a confidential relationship between the minor and a health care provider (e.g., physician asks adolescent's parent if the physician can talk with the child confidentially about a condition and the parent agrees).

E. **Rights/Restrictions of Personal Representative.** The Personal Representative must be treated as the Individual, except as follows:

1. The City of Sheboygan reasonably believes that the Individual has been or may be subjected to domestic violence, abuse, or neglect by the person seeking to be treated as a Personal Representative, or that treating the person as the Personal Representative could endanger the Individual;

2. The City of Sheboygan, in the exercise of professional judgment, decides that treating the person as the Individual's Personal Representative would not be in the Individual's best interest;

3. If a parent is the Personal Representative of a minor child, but Disclosure to the parent is prohibited under state law; or

4. Any of the exceptions outlined in Section 4.D above.

F. **Documentation.** The City of Sheboygan shall maintain documentation required under this Policy and Procedure consistent with the Retention of HIPAA Documentation Policy and Procedure.

G. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.502(g) – Uses and disclosures of protected health information: General rules, Personal Representatives Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

V. USES AND DISCLOSURES OF PHI TO PERSONS INVOLVED IN THE INDIVIDUAL'S CARE AND FOR NOTIFICATION PURPOSES

1. PURPOSE

To establish the City of Sheboygan's policy and identify the procedures for Use or Disclosure of PHI to persons involved in the Individual's care and for notification purposes.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan may generally Disclose PHI to a family member, other relative, close friend, or any other person identified by the Individual if the Disclosure is directly relevant to that person's involvement with the Individual's care or Payment for care or to notify that person of the Individual's location, general condition, or death.

4. PROCEDURE

A. Uses and Disclosures of PHI to Persons Involved in the Individual's Care.

1. Conditions for Disclosure if the Individual is Present. If the Individual is present for, or otherwise available, prior to a permitted Disclosure under this Manual, then the City of Sheboygan may Disclose the PHI only if it:

    a. Obtains the Individual's agreement;

    b. Provides the Individual with the opportunity to object to the Disclosure, and the Individual does not express an objection (this opportunity to object and the Individual's response may be done orally); or

    c. May reasonably infer from the circumstances, based on the exercise of professional judgment, that the Individual does not object to the Disclosure.

2. Conditions for Disclosure if the Individual is Not Present or is Incapacitated. The City of Sheboygan may, in the exercise of professional judgment, determine whether the Disclosure is in the best interest of the Individual, and, if so, Disclose only that PHI which is directly relevant to the person's involvement with the Individual's care if:

    a. The Individual is not present;

b. The opportunity to agree/object to the Use or Disclosure cannot practicably be provided because of the Individual's incapacity; or

c. In an emergency.

3. Conditions for Disclosure for Disaster Relief Purposes. The City of Sheboygan may Use or Disclosure PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating with such entities the Uses and Disclosures of PHI for notification purposes (as outlined in V.4.B below.)

4. Conditions for Disclosure if the Individual is Deceased. The City of Sheboygan may Disclose PHI to a person involved in the Individual's care or Payment for health care prior to the Individual's death if such PHI is relevant to such persons involved, unless doing so is inconsistent with any prior expressed preference of the Individual that is known to the City of Sheboygan.

5. Confirming Identity. The City of Sheboygan shall take reasonable steps to confirm the identity of an Individual's family member or friend. The City of Sheboygan is permitted to rely on the circumstances as confirmation of involvement in care.

B. **Uses and Disclosures of PHI for Notification Purposes.** The City of Sheboygan may Use or Disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a Personal Representative of the Individual, or another person responsible for the care of the Individual of the Individual's location, general condition, or death.

C. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.510(b) – Uses and disclosures for involvement in the individual's care and notification purposes Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

VI. INCIDENTAL USES AND DISCLOSURES OF PHI

1. PURPOSE

To establish a policy and identify procedures to ensure that the Use and Disclosure of PHI is made consistent with applicable law, regulations, and health information standards. The City of Sheboygan intends to limit incidental Uses and Disclosures of PHI and have in place reasonable safeguards where applicable.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

Many customary health care communications and practices play an important or even essential role in ensuring that Individuals receive prompt and effective care. Due to the nature of these communications and practices, as well as the various environments in which Individuals receive health care or other services from the City of Sheboygan, the City of Sheboygan recognizes that the potential exists for an Individual's health information to be Disclosed incidentally.

The City of Sheboygan is permitted to Use or Disclose PHI incident to a Use or Disclosure otherwise permitted or required by the Privacy Rule, provided that it has complied with the minimum necessary standard where required, the City of Sheboygan's Minimum Necessary Requirements Policy and Procedure, and the City of Sheboygan's Administrative Safeguards, Technical Safeguards, and Physical Safeguards to protect the privacy of PHI. The City of Sheboygan recognizes that an incidental Use or Disclosure that occurs as a result of a failure to apply reasonable Administrative Safeguards, Technical Safeguards, and Physical Safeguards or the minimum necessary standard, where required, is not permitted under the Privacy Rule.

4. PROCEDURE

A. **Incidental Uses and Disclosures of PHI.** The City of Sheboygan may Use or Disclose information that occurs as a by-product of an otherwise permissible Use or Disclosure as long as (i) the City of Sheboygan has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with regard to the primary Use or Disclosure and (ii) the incidental Use or Disclosure could not reasonably be prevented, was limited in nature, and occurred as a result of another Use or Disclosure permitted by the Privacy Rule.

B. **Reasonable Safeguards.** The City of Sheboygan shall also adopt reasonable Administrative Safeguards, Technical Safeguards, and Physical Safeguards to prevent Uses or Disclosures that are not permitted by the Privacy Rule as well as that limit incidental Uses or Disclosures.

C. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.502(a)(1)(iii) – Incident to a use or disclosure otherwise permitted Minimum Necessary Requirements Policy and Procedure The City of Sheboygan HIPAA Policies and Procedure Manual Volume 3 Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

VII. SALE OF PHI

1. PURPOSE

To establish the City of Sheboygan's policy and identify the procedures for Use and Disclosure of PHI that constitutes a Sale of PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

As Required by Law, the City of Sheboygan will secure an authorization for any Use or Disclosure of PHI that constitutes a Sale of PHI.

4. PROCEDURE

A. **Authorization Required.** Unless otherwise permitted by law, the City of Sheboygan will secure an Individual authorization for any Use or Disclosure of PHI that constitutes a Sale of PHI. The authorization must include a statement that the Disclosure will result in remuneration to the City of Sheboygan or the applicable third party.

B. **Authorization Not Required.** Sale of PHI does not include a Disclosure of PHI:

1. For public health purposes pursuant to the HIPAA Rules;

2. For Research purposes pursuant to the HIPAA Rules, where the only remuneration received by the City of Sheboygan or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

3. For Treatment and Payment purposes;

4. For the sale, transfer, merger, or consolidation of all or part of the City of Sheboygan and for related due diligence pursuant to the HIPAA Rules;

5. To or by a Business Associate for activities that the Business Associate undertakes on behalf of the City of Sheboygan pursuant to the HIPAA Rules, and the only remuneration provided is by the City of Sheboygan to the Business Associate for the performance of such activities;

6. To an Individual, when requested as access to PHI or an accounting of Disclosures of PHI pursuant to the HIPAA Rules (see Individual's Right to Access PHI Policy and Procedure and Accounting of Disclosures of PHI Policy and Procedure);

7. When Required by Law; and

8. For any other purpose permitted by and in accordance with HIPAA Rules, where the only remuneration received by the City of Sheboygan or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

C. **Business Associates.** Any BAAs that allow the Business Associate to engage in the Sale of PHI shall be approved by City Administrator .

D. **Documentation.** The City of Sheboygan shall maintain the Authorization for Use and Disclosure of PHI Form consistent with the Retention of HIPAA Documentation Policy and Procedure.

E. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.508(a)(4) – Authorization Required – Sale of protected health information Individual's Right to Access PHI Policy and Procedure Accounting of Disclosures of PHI Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Authorization for Use and Disclosure of PHI Form
Responsible Senior Leader	Privacy Officer
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

VIII. USES AND DISCLOSURES OF DE-IDENTIFIED DATA AND LIMITED DATA SETS

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures for the Use and Disclosure of De-identified Data and Limited Data Sets.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan may Use or Disclose a Limited Data Set, provided the recipient of such Limited Data Set enters into a Data Use Agreement.

The HIPAA Rules do not restrict The City of Sheboygan's Use or Disclosure of De-identified Data.

4. PROCEDURE

A. **Limited Data Sets.** The City of Sheboygan may Use or Disclose an Individual's PHI consistent with the Limited Data Sets and Data Use Agreements Policy and Procedures.

B. **De–identified Data.** The City of Sheboygan may Use or Disclose De-identified Data without obtaining an Individual's authorization. If the City of Sheboygan is creating De-identified Data, the City of Sheboygan shall follow the process for De-identification set out in the De-identification of PHI Policy and Procedure.

C. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.514(b) – De-Identification 45 C.F.R. § 164.514(e) – Limited Data Set Limited Data Sets and Data Use Agreements Policy and Procedures De-identification of PHI Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

IX. VERIFICATION OF IDENTITY AND AUTHORITY PRIOR TO DISCLOSURE OF PHI

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures to verify the identity of persons and entities requesting PHI and the authority of such persons or entities to access/receive PHI prior to Disclosing PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

Before Disclosing PHI, the City of Sheboygan shall verify the identity of the recipient and the recipient's authority to access/receive PHI, unless the identity and authority are known to the City of Sheboygan.

In addition, when it is a condition of Disclosure, prior to the Disclosure of PHI, the City of Sheboygan will obtain any documentation, statements, or representations of the recipient as required by the Privacy Rule.

4. PROCEDURE

A. **Verification of Identity and Authority.** Before Disclosing PHI, the City of Sheboygan will obtain sufficient information from the person requesting the PHI to logically conclude that the person's identity is valid and the person has authority to access/receive the PHI. The type of information required will depend on the nature of the request, from whom it is made, and the method in which it is made.

1. Request in Person.

a. When a request for PHI is made in person, the City of Sheboygan will generally verify identity by inspecting some form of photo identification. If photo identification is unavailable, the City of Sheboygan may verify identity by inspecting some other form of government-issued identification.

b. In cases of Disclosure for public policy purposes, authority to access/receive PHI may generally be verified by receipt of the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) of the subject of the PHI and:

i. A written statement of the authority under which the PHI is requested (or if a written statement is not available, a documented oral statement); or

ii. A legal document, such as a court order signed by a judge or other appropriate legal process meeting the requirements under the HIPAA Rules and state law.

2. Request By Telephone. When a request for PHI is made by telephone, the City of Sheboygan may generally verify identity by confirmation of information that identifies the person requesting the PHI. For example, if the person requesting the PHI is the subject of the PHI, then identity may be established by providing his/her full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number).

3. Request by Third Party. When the person requesting the PHI is a third party, the City of Sheboygan may verify identity by obtaining the caller's telephone number and calling him/her back, making sure the area code and exchange matches a listed telephone number for the third party. In order to verify authority to access/receive PHI when it is requested by someone other than the subject Individual, the City of Sheboygan will obtain the full name, date of birth, and one other additional piece of information (i.e., SSN, other identification number, address, or telephone number) regarding the subject of the PHI and a statement of the authority under which the PHI is requested. The City of Sheboygan is not required to release PHI when the request for release is made by telephone.

4. Request by Mail. If a request for PHI is received by mail, the City of Sheboygan may generally verify identity by receipt of some unique piece of information that identifies the person requesting the information or by receipt of the request in a format that tends to establish the identity of the person making the request. For example, if the person requesting the PHI is the subject of the PHI, then a written request containing the person's SSN or other unique identification number will be sufficient. When the person requesting the information is a health care provider or a public agency, receipt of the request on appropriate letterhead will be sufficient.

B. **Verification Documentation.** The person verifying the documentation, statements, or representations provided by the recipient as required by the Privacy Rule may, when doing so is reasonable under the circumstances, rely on documentation, statements, and representations that, on their face, meet the applicable requirements. Such reliance will not be reasonable when information is known by the person that tends to indicate the documentation, statement, or representation is not authentic. In such situations, additional steps to verify the authenticity of the documentation, statement, or representation shall be taken. The Privacy Officer will assist with any questions concerning appropriate verification of identity or authority to access/receive PHI.

C. **Log of Verifications.** The City of Sheboygan will keep a log of all verifications, which will include all information required to be obtained under this Policy. The

City of Sheboygan shall maintain the Log of Verifications consistent with the Retention of HIPAA Documentation Policy and Procedure.

D. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.508(b)– Valid Authorizations 45 C.F.R. § 164.514(h) – Verification Requirements Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Log of Verifications
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

X. MINIMUM NECESSARY REQUIREMENTS

1. PURPOSE

To help ensure that the City of Sheboygan Uses and Discloses only the minimum amount of PHI necessary for accomplishing the intended purpose.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

"Minimum Necessary" means the process that is outlined in the HIPAA Rules, i.e., when Using or Disclosing PHI or when requesting PHI from another entity, the City of Sheboygan must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the appropriate Use, Disclosure, or request.

3. POLICY

A. When Using, Disclosing or requesting PHI, the City of Sheboygan shall make reasonable efforts to limit the Use or Disclosure of PHI to the Minimum Necessary to accomplish the intended purpose of the appropriate requested Use or Disclosure.

B. **Exceptions.** The Minimum Necessary standard does not apply in the following circumstances:

1. Disclosures to a health care provider for Treatment;

2. Disclosures to the Individual or a Covered Entity upon the Individual's request;

3. Uses or Disclosures made pursuant to an authorization;

4. Disclosures to the Secretary and/or HHS for compliance and enforcement purposes;

5. As Required by Law; and

6. Uses or Disclosures required for compliance with the HIPAA Rules.

7. ***All other Uses and Disclosures are subject to the Minimum Necessary rule, and relevant Workforce members should verify the need for the Use or Disclosure of PHI to only that information necessary to accomplish the intended purposes of the Use of Disclosure.***

4. PROCEDURE

A. **De-Identified Data or Limited Data Set.** The City of Sheboygan will request, Use or Disclose De-Identified Data or a Limited Data Set when possible. Any

Disclosure of a Limited Data Set shall be in compliance with the Uses and Disclosures of De-identified Data and Limited Data Sets Policy and Procedure.

B. **Minimum Necessary.** If Use, request, or Disclosure of De-Identified Data or a Limited Data Set is not possible, the City of Sheboygan will not Use, request, or Disclose PHI that is more than the Minimum Necessary to accomplish the purpose of the Use, request, or Disclosure.

C. **Access to PHI.** The City of Sheboygan will allow only relevant Workforce members to have access to the Minimum Necessary PHI required by their job functions consistent with the City of Sheboygan's safeguards, including the Information System Activity Review Policy and Procedure; Information Access Management Policy and Procedure; Access Establishment, Modification and Review Policy and Procedure; Workstation Use Policy and Procedure; Workstation Security Policy and Procedure; Unique User Identification Policy and Procedure; Automatic Logoff Policy and Procedure; Person or Entity Authentication Policy and Procedure; and Integrity Controls Policy and Procedure.

D. **Disclosures of PHI.** The City of Sheboygan is often asked to Disclose PHI to other Covered Entities, regulatory agencies, law enforcement authorities and others. Many of these Disclosures are permitted or Required by Law and do not require authorization by the subject Individual. Other Disclosures may require authorization by the subject Individual. Except for the exceptions outlined above in Section X.3.B, the City of Sheboygan will apply the Minimum Necessary standard to all Disclosures.

E. **Routine and Recurring Disclosures.** The City of Sheboygan applies the below listed criteria to the below listed Disclosures that the City of Sheboygan makes on a routine and recurring basis. All other Disclosures shall be reviewed on a case-by-case basis as set forth in the "Non-Routine Disclosures" section below.

1. Routine and Recurring Disclosures. For any type of disclosure that the City of Sheboygan makes on a routine and recurring basis, the City of Sheboygan must implement procedures to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure

2. Criteria. For routine disclosures/requests, the City of Sheboygan has applied criteria to limit PHI to what is reasonably needed to accomplish the intended purpose of the request, Use or Disclosure and has created standards to be applied for all such routine Disclosures/requests.

F. **Non-Routine Disclosures.** Non-routine Disclosures/requests are (a) Disclosures or requests that are made occasionally or (b) routine types of Disclosures or requests that are made to organizations that do not routinely request or Disclose PHI to the City of Sheboygan. For each non-routine Disclosure/request, the City of Sheboygan applies criteria to limit PHI to what is reasonably needed to accomplish the intended purpose of the request, Use or Disclosure. Non-routine requests are evaluated on a case-by-case basis in accordance with the following criteria:

1. Evaluate Requestor. The City of Sheboygan will consider whether the requestor is an entity subject to HIPAA and familiar with the requirements to safeguard PHI.

2. Evaluate Request. The City of Sheboygan will consider what type and amount of PHI is being requested.

3. Is This a Minimum Necessary Request. The City of Sheboygan will consider whether it may rely on the requestor's request. The City of Sheboygan may rely on the judgment of the requestor as to the Minimum Necessary amount of information needed when the request is made by:

    a. A public official who states that the Disclosure is the Minimum Necessary;

    b. A Covered Entity that represents that the information requested is the Minimum Necessary for the stated purpose(s);

    c. A Workforce member or a Business Associate of the City of Sheboygan if he/she states that the information is the Minimum Necessary needed; or

    d. A requestor who has provided appropriate documentation from an IRB when requesting information for Research purposes.

G. **Workforce Responsibility.**

1. Workforce members may not Use, request, or Disclose any PHI that is more than the minimum necessary to accomplish the purpose of the appropriate Use, request, or Disclosure.

2. Workforce members are expected to limit Uses, requests, and Disclosures of PHI to that which is reasonably necessary for their specific job functions.

3. Workforce members will not be granted access to PHI of family members without documentation that no other Workforce member could conduct/complete the job duties requiring access to such PHI.

H. **Workforce Training.** All Workforce members shall receive periodic training on the Minimum Necessary standard and the City of Sheboygan's expectations.

I. **Questions.** Workforce members should consult with the Privacy Officer is there are questions related to whether or not a Use of Disclosure fits within the minimum necessary restrictions. The Privacy Officer will review the situation and determine what information is necessary to Use of Disclose.

J. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.502 – General Uses and Disclosures of PHI 45 C.F.R. § 164.512 – Uses and Disclosures Not Requiring Authorization 45 C.F.R. § 164.514(d) – Standard for Minimum Necessary Requirements Uses and Disclosures of De-identified Data and Limited Data Sets Policy and Procedure Information System Activity Review Policy and Procedure Information Access Management Policy and Procedure Access Establishment, Modification and Review Policy and Procedure Workstation Use Policy and Procedure Workstation Security Policy and Procedure Unique User Identification Policy and Procedure Automatic Logoff Policy and Procedure Person or Entity Authentication Policy and Procedure Integrity Controls Policy and Procedure Uses and Disclosures of PHI for Research Purposes Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	None
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XI. NOTICE OF PRIVACY PRACTICES

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures for preparing and updating the City of Sheboygan's Notice of Privacy Practices and providing Individuals with adequate notice of the Uses and Disclosures of PHI that may be made by the City of Sheboygan, and of the Individual's rights and the City of Sheboygan's legal duties with respect to PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

"More Stringent" means, in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification adopted under the HIPAA Rules, a state law that meets one or more of the following criteria:

A. With respect to a Use or Disclosure, the law prohibits or restricts a Use or Disclosure in circumstances under which such Use or Disclosure otherwise would be permitted under the HIPAA Rules, except if the Disclosure is: (i) required by the Secretary in connection with determining whether the City of Sheboygan is in compliance with the HIPAA Rules; or (ii) to the subject Individual.

B. With respect to the rights of the subject Individual regarding access to or amendment of PHI, the law permits greater rights of access or amendment, as applicable.

C. With respect to information to be provided to the subject Individual about a Use, a Disclosure, rights, and remedies, the law provides the greater amount of information.

D. With respect to the form, substance, or the need for express legal permission from the subject Individual for Use or Disclosure of PHI, the law provides requirements that narrow the scope or duration, increases the privacy protections afforded (such as by expanding the criteria for), or reduces the coercive effect of the circumstances surrounding the express legal permission, as applicable.

E. With respect to recordkeeping or requirements relating to accounting of Disclosures, the law provides for the retention or reporting of more detailed information or for a longer duration.

F. With respect to any other matter, the law provides greater privacy protection for the subject Individual.

3. POLICY

Each Individual who is the subject of PHI must receive a Notice of Privacy Practices describing (1) the Uses and Disclosures of his/her PHI that may be made by or on behalf of the City of Sheboygan, (2) the Individual's rights, and (3) the City of Sheboygan's legal duties with respect to the Individual's PHI.

A Notice of Privacy Practices will be provided to Individuals at the time of first service delivery, within sixty (60) days after a material change, or upon request. the City of Sheboygan will also provide a notice of the availability of the Notice of Privacy Practices at least every three years.

4. PROCEDURE

A. **Individuals Receiving Notice of Privacy Practices.** All Individuals will receive the Notice of Privacy Practices as set forth in this Policy and Procedure, except inmates do not have a right to a Notice of Privacy Practices.

B. **Form of Notice of Privacy Practices.** The City of Sheboygan's Notice of Privacy Practices must be prepared in easy-to-read language and contain, as a minimum, the following elements:

1. The following statement as a header or in an otherwise prominent location: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

2. A description, including at least one example, of the types of Uses and Disclosures that the City of Sheboygan is permitted to make for purposes of Treatment, Payment, and Health Care Operations, with sufficient detail to place an Individual on notice of the Uses and Disclosures permitted or required;

3. A description of each of the other purposes for which the City of Sheboygan is permitted or required to Use or Disclose PHI without the Individual's authorization, with sufficient detail to place an Individual on notice of the Uses and Disclosures permitted or required;

4. If a Use or Disclosure for any purpose authorized by the HIPAA Rules is prohibited or materially limited by other applicable law (e.g., state law or 42 C.F.R. Part 2), the description of such Use or Disclosure must reflect the More Stringent law;

5. A description of the types of Uses and Disclosures that require an authorization (e.g., Sale of PHI);

6. A statement that the authorization may be revoked in accordance with the Authorization for Use and Disclosure of PHI Policy;

7. If the City of Sheboygan is going to engage in Fundraising communications, a statement regarding the Individual's opt-out rights consistent with the Uses and Disclosures of PHI for Fundraising Policy and Procedure;

8. A statement of the Individual's rights with respect to his/her PHI and how the Individual may exercise those rights, including:

   a. The right to request restrictions on certain Uses/Disclosures of PHI, and the fact that the City of Sheboygan does not have to agree to such restrictions,

   b. The right to receive confidential communications of PHI,

   c. The right to inspect and copy PHI,

   d. The right to amend PHI,

   e. The right to receive an accounting of Disclosures of PHI, and

   f. The right to receive a paper copy of the privacy notice upon request;

9. A statement that the City of Sheboygan is Required by Law to maintain the privacy of PHI, to provide Individuals with notice of the City of Sheboygan's legal duties and privacy practices with respect to PHI, and to notify affected Individuals following a Breach of Unsecured PHI;

10. A statement that the City of Sheboygan is required to abide by the terms of the Notice of Privacy Practices currently in effect;

11. For the City of Sheboygan to apply a change in a privacy practice that is described in the Notice of Privacy Practices to PHI that the City of Sheboygan created or received prior to issuing a revised Notice of Privacy Practices, a statement that the City of Sheboygan reserves the right to change the terms of the Notice of Privacy Practices and to make the new Notice of Privacy Practices provisions effective for all PHI that it maintains. This statement shall include a description of how the City of Sheboygan will provide individuals with a revised Notice of Privacy Practices;

12. A statement that Individuals may complain to the City of Sheboygan and to the Secretary about privacy rights violations, including a brief description of how Individuals may file a complaint with the City of Sheboygan, and a statement that Individuals will not be retaliated against for filing a complaint;

13. The name, or title, and telephone number of the City of Sheboygan's HIPAA Privacy Officer to contact for further information; and

14. The effective date of the Notice of Privacy Practices, which may not be earlier than the date printed or published.

C. **Availability of Notice of Privacy Practices.**

1. The Notice of Privacy Practices, or a summary of the notice, will be posted in a clear and prominent location (e.g., on a wall at one of the Designated Health Care Components).

2. The Notice of Privacy Practices will be prominently posted on the City of Sheboygan's website.

3. Individuals will receive a copy of the Notice of Privacy Practices at the time of their first appointment (including any services delivered electronically) or, in an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

4. Except in an emergency treatment situation, the City of Sheboygan will make a good faith effort to request that Individuals sign a Receipt of Notice of Privacy Practices Written Acknowledgement Form, though Individuals are not required to sign the acknowledgement to receive services. If the Individual does not sign the acknowledgement, the City of Sheboygan will document the refusal to sign and the reason for such refusal.

5. The acknowledgement of receipt or refusal to acknowledge receipt will be kept in the Individual's medical record.

6. The City of Sheboygan will promptly revise and distribute its Notice of Privacy Practices whenever there is a material change to the Uses or Disclosures, Individuals' rights, the City of Sheboygan's legal duties, or other privacy practices stated in the Notice of Privacy Practices.

7. Except where Required by Law, the City of Sheboygan will not implement a material change to any term of the Notice of Privacy Practices prior to the effective date of the Notice of Privacy Practices in which such material change is reflected.

8. Upon revision, the new versions of the Notice of Privacy Practices will be posted and used for distribution. It is not necessary to redistribute the Notices of Privacy Practices to Individuals who have received an older version.

D. **Electronic Notice.**

1. The City of Sheboygan may provide the Notice of Privacy Practices to an Individual by email, if the Individual agrees to such electronic notice and such agreement has not been withdrawn.

2. If the City of Sheboygan knows that the email transmission has failed, a paper copy of the Notice of Privacy Practices will be provided.

3. If the first service delivery to an Individual is delivered electronically, the City of Sheboygan shall provide the Notice of Privacy Practices automatically and contemporaneously in response to the Individual's first request for service.

E. **Workforce Responsibility.** All employees and Business Associates of the City of Sheboygan will treat an Individual's Protected Health Information consistent with the requirements of the Notice of Privacy Practices.

F. **Documentation.** The City of Sheboygan shall maintain its Notices of Privacy Practices and good faith efforts to obtain the Receipt of Notice of Privacy Practices Written Acknowledgement Form or documentation of refusal consistent with the Retention of HIPAA Documentation Policy and Procedure.

G. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.520 – Notice of Privacy Practices for PHI Uses and Disclosures of PHI for Fundraising Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Notice of Privacy Practices Receipt of Notice of Privacy Practices Written Acknowledgement Form
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XII. SPECIAL COMMUNICATION REQUIREMENTS

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures for special communications required to provide convenience for Individuals while preserving the privacy of PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan will permit Individuals to request to receive communication of PHI by alternative means or at alternative locations as long as the requests are reasonable.

For example: (1) An Individual may request that the City of Sheboygan contact him or her at work for appointment reminders rather than at home. The City of Sheboygan will honor that request if the Individual provides his or her work contact number; or (2) an Individual may request no voice mail messages, preferring contact only directly or in writing.

4. PROCEDURE

A. Request for Special Communications of PHI.

1. Request in Writing. Individuals may request to receive special communications from the City of Sheboygan. Requests to receive communications of PHI by alternative means or at alternative locations should be made in writing. The request should be in writing on the Request for Special Communications of PHI Form and forwarded to the Privacy Officer and City Administrator for review and processing.

2. Timing of Request. The Individual may request to receive communications of PHI by alternative means or at alternative locations at the time of admission, visit, or at any time during the course of their care.

B. Accommodation of Request for Special Communications of PHI.

1. The City of Sheboygan will accommodate all reasonable requests. The City of Sheboygan determines whether a request is reasonable based on the administrative difficulty of accommodating the request.

2. The City of Sheboygan will not require the Individual to provide a reason for the request. If the Individual does provide a reason, the City of Sheboygan will not deny a request based on whether the City of Sheboygan considers the given reason to be a good reason for making the request.

3. The City of Sheboygan may deny an Individual's request if the Individual does not specify an alternative address or other method of contact, or the Individual does not provide information as to how payment, if applicable, will be handled.

4. The Individual will be notified of the City of Sheboygan's decision whether to grant a request for confidential communications.

5. Requests will be honored until revoked unless otherwise specified by the Individual.

6. Upon granting a request, the appropriate Workforce members shall be provided with the communication requirements and are required to adhere to them.

C. **Documentation.** The City of Sheboygan will document the decision and action taken. The City of Sheboygan shall maintain the Request for Special Communications of PHI Form consistent with the Retention of HIPAA Documentation Policy and Procedure.

D. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on The City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.522 – Confidential Communications Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Request for Special Communications of PHI Form Revocation Form
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XIII. DESIGNATED RECORD SETS

1. PURPOSE

To establish the City of Sheboygan's policy and identify procedures for privacy requirements and criteria for identifying categories of records that will become an Individual's Designated Record Set.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

Individuals have a right to inspect, amend, and obtain copies of PHI that is contained in a Designated Record Set. The City of Sheboygan defines the Designated Record Set and maintains all PHI in the Designated Record Set in accordance with HIPAA.

4. PROCEDURE

A. Defining the Designated Record Set.

1. The Designated Record Set includes medical and billing records and other records that are used in whole or in part by the City of Sheboygan to make decisions about Individuals. This includes records that are used to make decisions about Individuals, whether or not the records have been used to make a decision about the particular Individual requesting access. This includes both paper and electronic records and systems.

2. External records are those records that were not created by or originated at the City of Sheboygan (e.g., records (notes, reports) Individuals bring from a non-City of Sheboygan provider). If external records are used to make health care decisions about an Individual, then those records are part of the Designated Record Set.

3. Examples of records included in the Designated Record Set:

    a. History and physical examinations and reports
    b. Progress notes
    c. Vital signs
    d. Psychiatric assessments and evaluations
    e. Photographs or videos
    f. Authorizations and consents (including research consents)
    g. Billing records
    h. Other records used to make health care decisions about individuals (e.g., other diagnostic tests and results, interpretative reports)

4. Records contained in an electronic medical record will be presumed to be available for Use in making decisions about an Individual, and therefore included in the Designated Record Set.

5. Records that otherwise meet the definition of Designated Record Set but are held by the City of Sheboygan Business Associate are also part of the Designated Record Set.

B. **Maintaining the Designated Record Set.** The City of Sheboygan shall maintain an Individual's Designated Records Set in compliance with the HIPAA Rules.

C. **Excluded from the Designated Record Set.** The following records are excluded from the City of Sheboygan's Designated Record Set and the Individual does not have a right to access these records for any purpose:

1. Personal notes and observations about the Individual created by health care providers provided that such notes are not included in the health record
2. PHI that is compiled in reasonable anticipation of, or for use in a civil, criminal or administrative action or proceeding
3. Quality assessment records
4. Credentialing records
5. Peer review files
6. Incident reports
7. Internal grievance reports
8. Information contained in employee records
9. Information contained in the servers of a health information exchange in which the City of Sheboygan participates that has not been integrated into a Designated Record Set
10. Financial reports used for Health Care Operations
11. Coding queries
12. Internal compliance reports and audits
13. Administrative records
14. Attorney-client privileged records, or any other record that is subject to privilege under state and/or federal law
15. Public health records and statistical data
16. Temporary notes or worksheets
17. Research records that are not Used or are not available (to the treating provider) to make health care decisions about an Individual
18. Any other record that is not used to make a health care decision about the Individual

D. **Documentation.** The City of Sheboygan shall maintain the Designated Record Set consistent with the Retention of HIPAA Documentation Policy and Procedure.

E. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.501 – Designated record set definition 45 C.F.R. § 164.524(a) – Access to Protected Health Information 45 C.F.R. § 164.526(a) – Right to Amend Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XIV. INDIVIDUAL'S RIGHT TO ACCESS PHI

1. PURPOSE

To provide a consistent process to honor an Individual's right to inspect and access his/her PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

A. **Right to Access PHI.** The City of Sheboygan will provide Individuals, upon request, with access to the PHI about the Individual in a Designated Record Set maintained by or for the City of Sheboygan. This includes the right to inspect or obtain a copy (or both) of the PHI as well as to direct the City of Sheboygan to transmit a copy to a designated person or entity of the Individual's choice. The City of Sheboygan will provide Individuals with access to this PHI for as long as the PHI is maintained by or for the City of Sheboygan regardless of the date the PHI was created, whether the PHI is maintained in paper or electronic systems onsite, remotely, or archived, or where the PHI originated.

The City of Sheboygan will not impose unreasonable measures on an Individual requesting access that serve as barriers to or unreasonably delay the Individual from obtaining access. For example, the City of Sheboygan will not require an Individual (i) who wants a copy of his/her record mailed to her home address to physically come to the City of Sheboygan's office to request access and provide proof of identity in person; (ii) to use a web portal for requesting access; or (iii) to mail an access request.

B. **No Right of Access to PHI.** An Individual does not have a right to inspect and copy the following information:

1. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

2. PHI maintained by the City of Sheboygan that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 263a ("CLIA"), or exempt from CLIA pursuant to 42 C.F.R. § 493.3. In other words, PHI generated by:

   a. Facilities or facility components that perform testing for forensic purposes.

   b. Research laboratories that test human specimens but do not report Individual-specific results for diagnosis, prevention, Treatment, or the assessment of the health of Individuals.

c. Laboratories certified by the National Institutes on Drug Abuse ("NIDA") in which drug testing is performed that meets NIDA guidelines and regulations.

4. PROCEDURE

A. **Requests for Access.** The City of Sheboygan requires Individuals to request access in writing. The City of Sheboygan offers Individuals the Request for Access to Own PHI Form, as the City of Sheboygan has determined that use of this form does not create a barrier to or unreasonably delay the Individual from obtaining access to PHI. However, the Individual may forgo the City of Sheboygan's Request for Access to Own PHI Form as long as the Individual's written request provides the information minimally necessary for the City of Sheboygan to understand the request, verify the Individual's identity, and review/respond to the request.

B. **Processing an Individual's Request for Access to PHI.** The City of Sheboygan will determine the accessibility of the PHI based on the criteria included in this Policy and Procedure, state and federal laws, and the availability of PHI.

1. Timing of Review. The City of Sheboygan will take action as soon as possible and within thirty (30) days after receipt of the request with one 30-day extension permitted as needed to respond. The City of Sheboygan may need up to sixty (60) days to respond when the PHI is off-site. The City of Sheboygan will provide the Individual with a written statement of the reasons for the delay and the date by which the access request will be processed.

2. Verification. The City of Sheboygan will take reasonable steps to verify the identity of the Individual making a request for access, but the verification processes and measures will not create barriers to or unreasonably delay the Individual from obtaining access to his/her PHI.

3. Personal Representatives. An Individual's Personal Representative has the right to access PHI about the Individual in a Designated Record Set (as well as direct the City of Sheboygan to transmit a copy of the PHI to a third party of the Individual's choice) consistent with the HIPAA Rules and this Policy and Procedure.

4. Individual Right to Direct PHI to Another Person. An Individual has the right to direct the City of Sheboygan to transmit PHI about the Individual directly to a third party of the Individual's choice. The Individual's request to direct the PHI to another person must be in writing, signed by the Individual, and clearly identify the designated person and where to send the PHI. The same requirements for providing the PHI to the Individual, such as the fee limitations and requirements for providing the PHI in the form and format and manner requested by the Individual, apply when an Individual directs that the PHI be sent to another person. However, these Individual-initiated requests are processed differently than requests

received from third parties accompanied by an authorization signed by the Individual, which do not have the same fee limitations and requirements for providing the PHI.

C. **Granting Access.** The Individual will be allowed to access the PHI in the form requested by the Individual if the PHI is readily producible in that form. If not, it will be provided in a form agreed upon by both the City of Sheboygan and the Individual.

1. Where an Individual requests an electronic copy of PHI that the City of Sheboygan maintains only in paper, the City of Sheboygan will provide the Individual with an electronic copy if it is readily producible electronically and in the electronic format requested if readily producible in that format, or if not, in a readable alternative electronic format or hard copy format agreed to by the City of Sheboygan and the Individual.

2. Where an Individual requests an electronic copy of PHI that the City of Sheboygan maintains electronically, the City of Sheboygan will provide the Individual with access to the PHI in the requested electronic form and format, if readily producible. When the PHI is not readily producible in the electronic form and format requested, the City of Sheboygan will provide access to an agreed upon alternative readable electronic format.

3. Whether a particular mode of transmission or transfer is readily producible will be based on the City of Sheboygan's capabilities and the level of security risk that the mode of transmission or transfer may introduce to the PHI on the City of Sheboygan's systems (as opposed to security risks to the PHI once it has left the systems). The City of Sheboygan will not tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the Individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the City of Sheboygan's Security Rule risk analysis. The City of Sheboygan does have the capability to transmit PHI by mail or email (except in the limited case where email cannot accommodate the file size of the requested files).

4. The City of Sheboygan may provide the Individual with a summary or explanation of the requested PHI if the Individual agrees in advance to the summary or explanation and agrees to any fees charged for creating the summary or explanation.

5. The Individual may make an appointment during normal business hours to inspect or obtain a copy of the PHI, or the City of Sheboygan will mail a copy at the Individual's request. The City Administrator or designee may need to discuss the scope, format, or other issues related to the request with the Individual to help provide access to the correct information.

6. The City of Sheboygan may charge a reasonable, cost-based fee for copying, postage, and preparation of a summary or explanation. The fee will include only the cost of:

    a. Labor for copying the PHI requested by the Individual, whether in paper or electronic form;

    b. Supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the Individual requests that the electronic copy be provided on portable media;

    c. Postage, when the Individual requests that the copy, or the summary or explanation, be mailed; and

    d. Preparation of an explanation or summary of the PHI, if agreed to by the Individual.

    The fee will not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by state law.

7. The City of Sheboygan will provide the PHI, costs, and summary or explanation if applicable, on the Grant of Request for Access to Own PHI Form.

8. If the Individual feels the PHI is inaccurate, the Individual may request to amend the PHI, consistent with the Amendment of PHI Policy and Procedure.

D. **Denying Access.**

1. If The City of Sheboygan denies access, in whole or in part, to the PHI, the Individual will be given: a written denial on the Denial of Request for Access to Own PHI Form explaining why the City of Sheboygan denied access and stating how the Individual can have this denial reviewed, access to any other PHI requested (after excluding the PHI to which access is denied), and information pertaining to the City of Sheboygan's privacy and PHI complaint process.

2. If The City of Sheboygan does not maintain the PHI that was requested by the Individual and the City of Sheboygan knows where the information is kept, the City of Sheboygan will inform the Individual where to seek the information.

3. If access is denied on grounds permitted under HIPAA, the Individual has the right to have the denial reviewed as set forth in this Policy and Procedure.

E. **Denials Not Subject to Further Review.** The City of Sheboygan may deny an Individual access to his or her PHI without providing the Individual an opportunity for review of the decision when the reason for the denial is any of the following:

1. The information requested is the type of information listed in the three exceptions stated above.

2. The City of Sheboygan is acting under direction of a correctional institution and access to the information would jeopardize the health, safety, security, custody, or rehabilitation of the Individual who is an inmate or of other inmates, the safety of any officer, employee, or other person at the correctional institution, or any person responsible for transporting the Individual who is an inmate.

3. The Individual is taking part in certain Research studies and has temporarily waived this right for the duration of the Research study.

4. The PHI is contained in records that are subject to the Privacy Act, 5 U.S.C. § 522a (i.e., certain records under the control of a federal agency, which may be maintained by a federal agency or a contractor to a federal agency).

5. The PHI was obtained from someone other than the City of Sheboygan under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

F. **Denials Subject to Further Review.**

1. Individuals may have denials of access reviewed when the reason for denial is any of the following:

   a. A licensed health care professional has determined, in exercising professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Individual or another person.

   b. The PHI makes reference to another person (unless the other person is a health care provider) and a licensed health care professional has determined, in exercising professional judgment, that the access requested is reasonably likely to cause substantial harm to the other person.

   c. The request for access is made by the Individual's Personal Representative, and a licensed health care professional has determined, in exercising professional judgment, that the provision of access to the Personal Representative is reasonably likely to cause substantial harm to the Individual or another person.

2. If access is denied for any of these reasons, the Individual must initiate a written request to have the denial reviewed by a licensed health care

professional who is designed by the HIPAA Privacy Officer or designee to act as a reviewing official and who did not participate in the original decision to deny access, who will make the determination within a reasonable period of time. The City of Sheboygan will promptly provide written notice to the Individual of the determination of the reviewing professional.

G. **Documentation.** The City of Sheboygan shall maintain an Individual's Request for Access to Own PHI, Grant of Request for Access to Own PHI, Denial of Request for Access to Own PHI, written requests for review of denials, and any other records resulting from an Individual's request for access to his or her own PHI consistent with the Retention of HIPAA Documentation Policy and Procedure.

H. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.524 – Access of individuals to protected health information 45 C.F.R. § 164.501 – Designated record set definition Amendment of PHI Policy and Procedure Risk Analysis and Risk Management Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Request for Access to Own PHI Grant of Request for Access to Own PHI Denial of Request for Access to Own PHI
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XV. AMENDMENT OF PHI

1. PURPOSE

This Policy establishes the City of Sheboygan's policy and outlines procedures for reviewing and processing requests for amendments to PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan honors Individuals' rights to request an amendment or correction to PHI for as long as that information is maintained in a Designated Record Set for or on behalf of the City of Sheboygan.

4. PROCEDURE

A. Requests for Amendment of PHI.

1. Written Request. All requests for amendments to PHI must be submitted to the Security Officer in writing. The City of Sheboygan offers the Request for Amendment of PHI Form, but the City of Sheboygan will honor all requests that clearly identify the PHI to be amended as well as the reasons for the amendment.

2. Time Frame for Acting Upon Request for Amendments. The City of Sheboygan will act upon the Individual's request for an amendment no later than sixty (60) days after receipt of such request. If the City of Sheboygan is unable to act upon the request within the 60-day period, the Individual will be provided with a written notice of the reasons for the delay and the date by which the City of Sheboygan will complete such action. In no case will such extension extend beyond thirty (30) days. Notwithstanding the foregoing, however, if the request for amendment is for "treatment records" created under Wis. Stat. § 51.30, the City of Sheboygan must act on the request no later than 30 days (without any available extensions).

B. Processing of Request for Amendment of PHI.

1. Reasons for Denials of Amendment Requests. Requests may be denied if the PHI requested for amendment:

   a. Was not created by the City of Sheboygan, unless the originator is no longer available to act on the request;

   b. Is not part of the Designated Record Set;

c. Is not accessible to the Individual because federal and state law does not permit it; or

d. Is accurate and complete as determined by the City of Sheboygan upon review.

2. Denial of Amendment Requests. If the City of Sheboygan denies a requested amendment, completely or in part, the City of Sheboygan will:

a. Notify the Individual in writing using the Denial of Amendment of PHI Request Form about the denial to make an amendment to his/her PHI. Denial will include the following information:

i. The reason(s) for the denial.

ii. The notice must describe the Individual's right to submit a written statement disagreeing with the denial and how the Individual may file such a statement.

iii. A statement notifying the Individual that, if the Individual does not submit a statement of disagreement, the Individual may request that the City of Sheboygan provide the request for amendment and the denial with any future disclosures of the PHI.

iv. If the Individual submits a "statement of disagreement," the City of Sheboygan may prepare a written rebuttal statement to the Individual's statement of disagreement. The statement of disagreement will be appended to the PHI or, at the City of Sheboygan's option, a summary of the disagreement will be appended, along with the rebuttal statement of the City of Sheboygan.

v. Information relative to how the Individual may file a complaint with the HIPAA Privacy Officer or to the Secretary.

b. The notice to the Individual must include the name, title, and telephone number of the contact person or office designated to receive complaints.

3. Acceptance of Amendment Requests. If the request is granted, the City of Sheboygan will:

a. Insert the amendment or provide a link within the Designated Record Set to the amendment at the site of the information that is the subject of the request for amendment;

b. Inform the Individual that the amendment is accepted using the Grant of Amendment of PHI Request Form;

c. Obtain the Individual's identification of an agreement to have the City of Sheboygan notify the relevant persons with whom the amendment needs to be shared; and

d. Within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the Individual, and persons, including Business Associates, that the City of Sheboygan knows have the PHI that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the Individual.

C. **Documentation.** the City of Sheboygan shall maintain an Individual's Request for Amendment of PHI, Grant of Request for Amendment of PHI, Denial of Request for Amendment of PHI, written requests for review of denials, and any other records resulting from an Individual's request for amendment of PHI consistent with the Retention of HIPAA Documentation Policy and Procedure.

D. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.526 – Amendment of protected health information
Attachments	Request for Amendment of PHI Grant of Amendment of PHI Denial of Amendment of PHI Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XVI. ACCOUNTING OF DISCLOSURES OF PHI

1. PURPOSE

To establish the City of Sheboygan's practice of maintaining an accounting of Disclosures of an Individual's PHI and outline how an Individual requests an accounting of Disclosures of his or her PHI, what information the City of Sheboygan provides, and how/when it is delivered to the Individual.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

The City of Sheboygan will maintain an accounting of Disclosures of PHI for each Individual in the form of the Accounting of Disclosures Log and provide an Individual with the right to receive an accounting of Disclosures of PHI as Required by Law.

4. PROCEDURE

A. **Requesting an Accounting of Disclosures.** An Individual may request an accounting of Disclosures of his/her PHI made by the City of Sheboygan, including any Business Associate on behalf the City of Sheboygan, during a specified time period of up to six (6) years prior to the date of the request of an accounting. Requests for an accounting of Disclosures should be directed to City Administrator, who shall be responsible for processing requests.

B. **Time Frame for Providing Accounting of Disclosures Data on Request.** An Individual's request for an accounting of Disclosures must be provided to the Individual or representative within 60 days of such request. If unable to provide the accounting within the 60-day time frame, a one-time 30-day extension may be provided if:

1. The Individual is notified in writing of the delay;

2. The notice includes the reason(s) why the delay is necessary; and

3. The notice includes the date by which the accounting will be provided.

C. **Cost of Providing an Accounting.** The City of Sheboygan will provide the first accounting in any 12-month period to an Individual without charge and may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same Individual within the 12-month period, provided that the City of Sheboygan informs the Individual in advance of the fee and provides the Individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

D. **Maintaining an Accounting of Disclosures.**

1. Tracking Disclosures. Disclosures must be tracked by the City of Sheboygan for purposes of an accounting except for the following Disclosures:

   a. To carry out Treatment, Payment, or Health Care Operations, as permitted under the HIPAA Rules.

   b. To the Individual about his/her own PHI.

   c. To persons involved in the Individual's care.

   d. As part of a Limited Data Set under a Data Use Agreement.

   e. For national security purposes.

   f. Pursuant to the Individual's authorization.

   g. To law enforcement or correctional institutions as provided under state law.

   h. To federal/health department officials as permitted under current law.

2. Time Frame for Accounting Reports. The accounting record must include Disclosures of PHI that occurred during the six years prior to the date of such request, including Disclosures made by or to any of the City of Sheboygan's Business Associates.

3. Accounting Records Content. The content of the written accounting of Disclosures record must contain, at a minimum, the following information:

   a. Date of the Disclosure.

   b. Name of the entity or Individual who received the PHI.

   c. The address of the person receiving the PHI (if known).

   d. A brief description of the PHI Disclosed.

   e. A brief statement of the purpose of the Disclosure or a copy of the Individual's authorization or the request for the Disclosure.

E. **Multiple Disclosures.** If, during the time period for the accounting, multiple Disclosures have been made to the same entity or Individual for a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth in Section 4.D.3 of this Policy and Procedure for the first Disclosure, and then summarize the frequency and number of Disclosures made during the accounting period and the date of the last Disclosure during the accounting period.

F. **Suspension of Right to an Accounting.** The City of Sheboygan will temporarily suspend an Individual's right to receive an accounting of Disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the City of Sheboygan with a written statement that:

1. Such an accounting to the Individual would be reasonably likely to impede the agency's activities, and

2. Specifying the time for which such a suspension is required.

Such requests made orally must be documented, including the identity of the agency or official making the request, and are limited to 30 days unless or until a written statement is provided.

G. **Log of Disclosures.** The City of Sheboygan will keep a log of all Disclosures required above which will include all necessary information in the form of the Accounting of Disclosures Log. The City of Sheboygan shall maintain the Accounting of Disclosures Log and Request for Accounting of Disclosures of PHI consistent with the Retention of HIPAA Documentation Policy and Procedure.

H. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.528 – Accounting of disclosures of protected health information Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Request for Accounting of Disclosures of PHI Accounting of Disclosures Log
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

XVII. INDIVIDUAL'S RIGHT TO REQUEST RESTRICTIONS ON CERTAIN USES AND DISCLOSURES OF PHI

1. PURPOSE

To establish the City of Sheboygan's practice of responding to Individuals' requests for restrictions on certain Uses and Disclosures of PHI.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

A. **Individual Request for Restrictions on Use and Disclosures of PHI.** The City of Sheboygan will take appropriate steps to protect and restrict the PHI created, received, maintained, and transmitted by the City of Sheboygan. An Individual may request certain additional restrictions on how the City of Sheboygan archives or manages his/her PHI. The City of Sheboygan may agree to such requested restrictions if it believes the restriction will not limit its ability to provide quality health care Treatment, obtain Payment, or manage its Health Care Operations, and if its information systems and procedures will permit it to comply consistently with the requested restrictions.

B. **Granting Restriction Requests.** Except as otherwise Required by Law, the City of Sheboygan will agree to restriction requests related to Disclosures of PHI to a Health Plan when such Disclosures are for the purpose of carrying out Payment or Health Care Operations and the PHI pertains only to health care for which the costs have been paid out-of-pocket in full (by the Individual or on the Individual's behalf).

4. PROCEDURE

A. **Right to Request Restrictions on Use and Disclosure of PHI.** An Individual has the right to request restrictions on Uses and Disclosures of his/her PHI using the Request for Restriction on Certain Uses and Disclosures of PHI Form. The City of Sheboygan is not required to agree to all requested restrictions.

B. **Acceptance of Request for Restrictions.** The City of Sheboygan will accept restrictions requested by an Individual when the City of Sheboygan:

1. Has been paid out-of-pocket in full for the health care items or services related to the restriction, and

    a. the requested restriction is limited to Disclosures to a Health Plan for the purposes of carrying out Payment or Health Care Operations related to that health care item or service;

b. the requested restriction is limited to Disclosures of PHI solely related to that health care item or service; and

c. the requested restriction is not for a service covered by Medicare or Medicaid or Workers' Compensation.

2. Has the administrative, physical, and technical capability of complying with the restriction, and

a. finds that Individual care will not be detrimentally affected; and

b. has assurance that the Individual's financial obligations will be met, if applicable, and believes that the Individual is in danger or is a public figure whose identity at the City of Sheboygan could be disruptive.

C. **Termination of Restrictions.** If The City of Sheboygan agrees to a restriction, it will not Use or Disclose PHI in violation of the restriction. The City of Sheboygan may terminate its agreement to a restriction if:

1. The Individual agrees to or requests the termination in writing.

2. The Individual orally agrees to the termination and the oral agreement is documented.

3. The City of Sheboygan informs the Individual of the termination, in which case the termination will only be effective for PHI created or received after the Individual is so informed.

D. **When Restrictions Will Not Prevent Use or Disclosures.** A restriction will not be effective to prevent Use or Disclosures: (1) that are necessary to provide the Individual with emergency Treatment; (2) to the Secretary for purposes of determining compliance with HIPAA; (3) for a facility directory, unless the Individual opts out of the directory listing; or (4) for which an authorization, or the opportunity to agree or object, is not required.

E. **Documentation.** The City of Sheboygan shall maintain an Individual's Request for Restriction on Certain Uses and Disclosures of PHI Form and the City of Sheboygan's Response to Request for Restriction on Certain Uses and Disclosures Form consistent with the Retention of HIPAA Documentation Policy and Procedure.

F. **Sanctions for Non-Compliance.** Workforce members who violate this Manual may be subject to disciplinary action for misconduct and/or performance based on the City of Sheboygan's Sanction and Discipline Policy and Procedure.

References	45 C.F.R. § 164.522(a) – Right of an individual to request restriction of uses and disclosures Sanction and Discipline Policy and Procedure
Attachments	Request for Restriction on Certain Uses and Disclosures of PHI Form Response to Request for Restriction on Certain Uses and Disclosures of PHI Form Revocation Form
Responsible Senior Leader	City Administrator
Effective Date	**November 4, 2024**
Review Dates	November 1st of even years
Revisions	

40979198_1.DOCX

THE CITY OF SHEBOYGAN
HIPAA POLICIES AND PROCEDURES MANUAL

VOLUME 3:
SECURITY POLICIES AND PROCEDURES

ADOPTED: _____

TABLE OF CONTENTS[1]

[1] *Exhibits are provided in a separate document.*

EXHIBIT 3-V-A: USER ACCESS TRACKING ATTACHMENT

EXHIBIT 3-V-B: CONFIDENTIALITY AND INFORMATION ACCESS AGREEMENT

I. RISK ANALYSIS AND RISK MANAGEMENT

1. PURPOSE

To establish the information security risk management process for The City of Sheboygan. The risk management process is intended to support and protect The City of Sheboygan and its ability to fulfill its mission and effectively and consistently protect The City of Sheboygan's information assets. To help ensure that adequate Administrative Safeguards, Physical Safeguards, and Technical Safeguards are in place for The City of Sheboygan's ePHI.

2. POLICY

A. It is the policy of The City of Sheboygan to conduct risk analyses of the potential threats and vulnerabilities to the Confidentiality, Integrity, and Availability of ePHI and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of The City of Sheboygan's information security program.

B. Risk analysis and risk management are recognized as important parts of The City of Sheboygan's security compliance program. At a minimum, they are completed in accordance with the risk analysis and risk management requirements in the Security Rule, which include evaluations in response to environmental or operational changes affecting the security of ePHI (e.g., identification of new security risks, adoption of new technology affecting ePHI).

1. To the extent possible, risk analyses are done throughout system life cycles, before the purchase or integration of new technologies and prior to changes made to Physical Safeguards, while integrating technology and making physical security changes, and into sustainment and monitoring of appropriate security controls.

2. Information system technologies affecting ePHI are not deployed unless the technology is widely used and generally accepted as stable, reliable, and fit for its intended purpose. Exceptions are made only if purchase commitments are preceded by both a risk analysis, as set forth in the procedures below, and the approval of the Security Officer.

3. The City of Sheboygan performs periodic technical and non-technical assessments of the Security Rule requirements in response to environmental or operational changes affecting the security of ePHI.

C. Risk is managed through the implementation of security controls that are dictated based on the level of sensitivity and/or value the information assets provide to the business as well as the level of risk to which those assets are subject:

Level	Classification	Description
3	Restricted	The highest level requiring the maximum-security controls. Release of such information would cause exceptionally grave damage to The City of Sheboygan (e.g., PHI).
2	Sensitive	Release of such information would cause undesirable effects to The City of Sheboygan, but would not materially impact The City of Sheboygan's financials or business performance (e.g., policies).
1	Unclassified	Such information cannot be labeled with any of the above classifications and is generally available for public disclosure (e.g., job postings).

(See Information Classification Questionnaire Exhibit.)

To the extent possible, The City of Sheboygan implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the Confidentiality, Integrity, and Availability of The City of Sheboygan's ePHI.

2. Protect against reasonably foreseeable or anticipated threats or hazards to the security or Integrity of this information.

3. Protect against any reasonably anticipated Uses or Disclosures of ePHI that are not permitted or required by HIPAA or HITECH.

4. Ensure compliance by Workforce members.

D. Any remaining (residual) risk after other risk controls have been applied requires sign off by the Security Officer.

E. All Workforce members are expected to fully cooperate with all persons charged with doing risk management work.

3. PROCEDURE

A. **Oversight.** The Security Officer or his/ her designee oversees the security risk analysis and risk management process, in coordination with the City Administrator.

B. **Risk Analysis.** The intent of completing a risk analysis is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The following steps are utilized to conduct a full risk analysis, unless a contractor/consulting organization is hired that utilizes a different and acceptable risk analysis approach. (See System Build/Change Control Policy and Procedure.) The output of this process helps to identify appropriate controls for reducing or eliminating risk.

1. Step 1. System Characterization.

   a. Identify where ePHI is created, received, maintained, processed, and transmitted. Consider policies, laws, remote workforce and telecommuters, movable media and mobile devices (*e.g.*, computers, laptops, removable media, and backup media).

   b. When changing, purchasing, or otherwise introducing new applications or technologies into the production environment:

      i. *See* System Build/Change Control Policy and Procedure.

      ii. Document the classification of the highest data criticality/data sensitivity level.

2. Step 2. Threat Identification. Identify and document potential threats (the potential for threat sources to successfully exercise a particular vulnerability). (*See* HIPAA Security Threat Source List.)

3. Step 3. Vulnerability Identification. Develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat sources. This step may include testing systems, penetration testing, etc. (Vulnerability assessments are completed as described in System Build/Change Control Policy and Procedure).

4. Step 4. Control Analysis. Document technical and non-technical controls (policies, procedures, physical security measures (*e.g.*, complete a physical walkthrough on The City of Sheboygan's data processing areas, locations containing infrastructure systems, Workstations, and other areas that contain restricted information), training, technical mechanisms and functionalities, insurance, etc.) that have been or will be implemented by The City of Sheboygan to minimize or eliminate the likelihood (or probability) of a threat source exploiting a vulnerability and reduce the impact of such an adverse event.

5. Step 5. Likelihood Determination. Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat source given the existing or planned security controls. Utilize a scoring mechanism, such as one in NIST Special Publication 800-30 – Guide for Conducting Risk Assessments; low (.1), medium (.5), or high (1). (*See* Risk Likelihood, Impact & Level Definitions – NIST SP 800-30.)

6. Step 6. Impact Analysis. Determine the level of adverse impact that would result from a threat source successfully exploiting a vulnerability. Factors to consider should include the importance to The City of Sheboygan's mission; sensitivity and criticality of the ePHI (value or importance); costs associated; and loss of Confidentiality, Integrity, and Availability of systems and data. Utilize a magnitude of impact rating, such as one in NIST

Special Publication 800-30 – Guide for Conducting Risk Assessments; low (10), medium (50), or high (100). (*See* Risk Likelihood, Impact & Level Definitions – NIST SP 800-30.)

7. Step 7. Risk Determination. Calculate a risk level. (Multiply the NIST SP 800-30 likelihood rating by the impact rating; Risk level of low (1-10), medium (>10-50) or high (>50-100).) This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised.

8. Step 8. Control Recommendations. Identify controls that could reduce or eliminate the identified risks to an acceptable level, as appropriate to The City of Sheboygan's operations. Factors to consider may include level of sensitivity and/or value or the information assets, level of risk to which assets are subject, effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

9. Step 9. Results Determination.

    a. Document results of the risk analysis, such as in a risk summary and risk mitigation implementation plan.

    b. Obtain written approval from the City Administrator (or designee) for decisions on policy, procedure, budget, system operational and management changes, as well as acceptance of remaining risk for systems that create, receive, maintain, transmit, or otherwise impact (i) restricted information or affect security controls or authentication systems, or (ii) sensitive and non-sensitive information.

C. Risk Mitigation. Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk analysis process to ensure the Confidentiality, Integrity and Availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of The City of Sheboygan, consistent with its goals and mission. The following steps may be utilized to make determinations of the appropriate controls to put into place. Some of the steps may also be utilized when purchasing, upgrading, or moving ePHI systems and other applications or technologies and as needed to assist in The City of Sheboygan's risk mitigation efforts.

Step 1. Prioritize Actions. Using results from Step 7 of the risk analysis and after obtaining approvals in Step 9, identify and sort top risks (vulnerability-threat pairs), such as from high to low.

1. Step 2. Evaluate Recommended Control Options. Review the recommended control(s) from Step 8 as well as alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, User acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. Select a "most appropriate" control option for each vulnerability-threat pair, and document reasons for not selecting other controls.

2. Step 3. Conduct Cost-Benefit Analysis. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application.

3. Step 4. Select Control(s). Taking into account the information and results from previous steps and any other important criteria, determine the best control(s) for reducing risks to the information systems and to the Confidentiality, Integrity, and Availability of ePHI. These controls may consist of a mix of Administrative Safeguards, Physical Safeguards, and/or Technical Safeguards.

4. Step 5. Assign Responsibility. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources (e.g., time, money, etc.) needed for the successful implementation of controls.

5. Step 6. Develop Safeguard Implementation Plan. Develop an overall implementation or action plan and have the Security Officer and City Administrator approve such plan.

6. Step 7. Implement Selected Controls. As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

    a. Document the date controls are put into place.

    b. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

    c. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

    d. Provide regular status reports to the appropriate leader and other key stakeholders as appropriate.

D. Risk Management Schedule. The two principal components of the risk management process (risk analysis and risk mitigation) are carried out according to the following schedule to ensure the continued adequacy and continuous improvement of The City of Sheboygan's information security program:

1. Scheduled Basis. Conduct an overall risk analysis of The City of Sheboygan's information system infrastructure and policies and procedures in place to safeguard the Confidentiality, Integrity, and Availability of ePHI at least every five (5) years.

2. Throughout a System's Development Life Cycle. From the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential security threats and vulnerabilities to a system are done (*e.g.*, when purchasing, upgrading, changing, or moving ePHI systems). (*See* System Build/Change Control Policy and Procedure.)

3. As Needed. A full or partial risk analysis in response to environmental or operational changes affecting the security of ePHI may be done (e.g., when experiencing a Security Incident, turnover in key Workforce members/management, or other events that impact how ePHI is stored or transmitted).

4. Risk Mitigation. To the extent possible, selected security controls are put into place as described in the risk mitigation implementation plan or other plan developed during the risk analysis process.

E. Documentation. The City of Sheboygan shall maintain documentation of all risk analyses and risk mitigation efforts, including decisions made on what controls to put into place as well as those to not put into place, consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(1)(i) – Security Management Process 45 C.F.R. § 164.308(a)(1)(ii)(A) – Risk Analysis 45 C.F.R. § 164.308(a)(1)(ii)(B) – Risk Management 45 C.F.R. § 164.308(a)(8) – Security Evaluation NIST Special Publication 800-30 – Guide for Conducting Risk Assessments System Build/Change Control Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Information Classification Questionnaire HIPAA Security Threat Source List Risk Likelihood, Impact & Level Definitions – NIST Special Publication 800-30 – Guide for Conducting Risk Assessments
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

II. SYSTEM BUILD/CHANGE CONTROL

1. PURPOSE

To establish overarching security safeguarding measures to safeguard the Confidentiality, Integrity and Availability of PHI when changing, purchasing, or otherwise introducing new applications or technologies into the production environment, including identifying criteria for validating systems to ensure they are configured securely and performing vulnerability assessments.

2. POLICY

It is the policy of The City of Sheboygan to protect the Confidentiality, Integrity, and Availability of PHI by defining security requirements for controlling additions and other changes to production systems through risk analysis, vulnerability assessments, planning, approval, communication, documentation, and separation of duties.

3. PROCEDURE

A. **System Configuration.** The City of Sheboygan configures all systems according to established and approved standards aligned with industry best practice, The City of Sheboygan's HIPAA Policies and Procedures Manual, and The City of Sheboygan's Information Technology Policy Manual.

B. **File Structures.** Consistent account naming, system naming, and file structures are used that promote User tracking and Access troubleshooting. System administrators must follow the system, User, and file naming conventions established by their Information Technology (IT) Department.

C. **Primary Function.** Only one primary function is implemented per server that stores or transmits PHI, and all unnecessary and insecure services or functions are disabled.

D. **Encryption.** All non-console administrative Access is encrypted.

E. **Baseline Standards.** The City of Sheboygan maintains baseline configuration standards for server, Workstation, and laptops. (See Information Technology Policy Manual.)

F. **Risk Analysis.** The City of Sheboygan performs a risk analysis to identify the risk associated with changes to production information systems. Written approval from the City Administrator is required for identified risks that are mitigated or accepted. (See Risk Analysis and Risk Management Policy and Procedure.)

G. **Separation of Duties.** Changes to software applications that process PHI are promoted to production by a person other than the release builder.

H. Routine Changes. Changes that are well-defined, performed regularly, introduce limited risk, and are pre-approved by the Security Officer require only appropriate notification to execute as routine changes. The City of Sheboygan will maintain documentation of the following:

1. The change plan (as described below);

2. Justification for it being a routine change;

3. Date and time change was made; and

4. Provide documentation to the Security Officer.

I. Emergency Changes.

1. Emergency changes may be made when immediate action is necessary to safeguard the security of PHI. These emergency change plans must be submitted to the Security Officer and other appropriate parties as expeditiously as circumstances allow, before or immediately after the change is made.

2. The Security Officer reviews all emergency changes. Whenever possible, the Security Officer will provide written (paper or e-mail) approval for emergency changes.

J. Change Plan.

1. Applications are tested in a separate test environment.

2. When changing, purchasing, or otherwise introducing new applications or technologies into the production environment, The City of Sheboygan will document it in a change plan (see above for routine and emergency changes). The following is included in the change plan:

    a. A change schedule, including the times and date of a proposed change, including any downtime that may occur;

    b. System functions;

    c. System lead(s);

    d. Classification of the highest data criticality/data sensitivity level (see Information Classification Questionnaire Exhibit of Risk Analysis and Risk Management Policy and Procedure);

    e. The scope of the change including any Users, departments, business services, or technical components affected by the change;

    f. A summary of the technical risk involved in the change;

g. A list and description of implementation steps for the change;

h. A test plan for operational functionality;

i. A back-out plan to return to the pre-change state;

j. A list of the people involved in performing the change and their roles; and

k. A change notification plan.

3. Change plans shall be approved (via paper or e-mail) by the Security Officer.

K. Vulnerability Assessments.

1. Frequency.

a. Vulnerability assessments are completed:

i. Before placing systems and applications with PHI into production;

ii. When legal, regulatory, or business obligations change, as appropriate; and

iii. In the case of a security compromise.

b. A vulnerability assessment is also conducted using a vulnerability scanner to ensure the security baseline of the system or application was not impacted when:

i. A system application change was applied;

ii. Patches are applied to systems or applications;

iii. A Workstation image is changed;

iv. Server changes may impact the security settings of the server; and

v. Moving systems or applications from a less secure environment (e.g., test, development, outside hosting party, etc.) to The City of Sheboygan's normal production environment.

2. Methods and Tools. The City of Sheboygan uses approved methods and tools depending on the type and perspective of the assessment.

3. Identified Weaknesses. If a vulnerability assessment identifies weaknesses, the Security Officer will work with the IT Department, Privacy Officer and City Administrator to remediate or accept findings and include actions taken in the final vulnerability assessment report. (*See* Risk Analysis and Risk Management Policy and Procedure.)

4. Vulnerability Assessment Report. The Workforce members and/or vendors performing the vulnerability assessment will complete a vulnerability assessment report for the Security Officer to review and approve. The report may only be shared with individuals authorized by the Security Officer.

5. Recommendations for Action. Upon completion of a vulnerability assessment and review of the vulnerability assessment report, The City of Sheboygan will consider recommendations for action.

L. Change Review. The Security Officer will review changes on a bi-annual basis to identify any trends in changes and take appropriate action for continuous improvement.

References	45 C.F.R. § 164.308(a)(1)(ii) – Risk Analysis and Risk Management Information Technology Policy Manual Risk Analysis and Risk Management Policy and Procedure Information Classification Questionnaire Exhibit Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

III. INFORMATION SYSTEM ACTIVITY REVIEW

1. PURPOSE

To establish procedures to regularly review records of activity on information systems containing ePHI along with implementation of appropriate hardware, software, or procedural auditing mechanisms.

2. POLICY

The City of Sheboygan will have procedures to regularly review records of information system activity containing ePHI (e.g., audit logs, Access reports, and Security Incident tracking reports).

3. PROCEDURE

A. The Security Officer or designee will periodically review records of activity on information systems containing ePHI. Records of activity may include, but are not limited to:

1. Audit logs;
2. Access reports; and
3. Security Incident tracking reports.

B. Appropriate hardware, software, or procedural auditing mechanisms may provide the following information:

1. Date and time of activity;
2. Origin of activity;
3. Identification of User performing activity; and
4. Description of attempted or completed activity.

C. The level and type of auditing mechanisms to be used will be determined by The City of Sheboygan's risk analysis process. (*See* Information System Activity Review Audit Process Policy and Procedure.) Auditable events can include, but are not limited to:

1. Access of sensitive data (e.g., HIV test results, alcohol and other drug abuse records);
2. Use of a privileged account;
3. Information system startup or stop;

4. Failed authentication attempts; or

5. Security Incidents.

D. Records of activity created by audit mechanisms will be reviewed regularly by the Security Officer.

E. The City of Sheboygan's Workforce members should not monitor or review activity related to their own User accounts.

References	45 C.F.R. § 164.308(a)(1)(ii)(D) – Information System Activity Review Information System Activity Review Audit Process Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

IV. INFORMATION SYSTEM ACTIVITY REVIEW AUDIT PROCESS

1. PURPOSE

To establish procedures to audit Safeguards which monitor Access and activity to detect, report and guard against: network vulnerabilities and intrusions; breaches in Confidentiality and security of PHI; performance problems and flaws in applications; and improper alteration or destruction of ePHI (information integrity).

This Policy is applicable to The City of Sheboygan's information applications, systems, networks, and any computing devices, regardless of ownership (e.g., owned, leased, contracted, and/or stand-alone).

2. POLICY

The City of Sheboygan shall audit Access and activity of ePHI applications, systems, and networks and address standards set forth by the Security Rule to ensure compliance to safeguard the privacy and security of ePHI.

3. PROCEDURE

A. **Audit Responsibility.** Responsibility for auditing information system Access and activity is assigned to the Security Officer or other designee as determined by The City of Sheboygan's Security Officer. The Security Officer shall:

1. Assign the task of generating reports for audit activities to the individual responsible for the application, system, or network;

2. Assign the task of reviewing the audit reports to the individual responsible for the application, system, or network or any other individual determined to be appropriate for the task; and

3. Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).

B. **Auditing Processes.** Auditing processes may address date and time of each log-on attempt, date and time of each logoff attempt, devices used, functions performed, etc.

1. User: User level audit trails generally monitor and log all commands directly initiated by the User, all identification and authentication attempts, and files and resources Accessed.

2. Application: Application level audit trails generally monitor and log User activities, including data files opened and closed, specific actions, and printing reports.

3. System: System level audit trails generally monitor and log User activities, applications Accessed, and other system defined specific actions.

4. Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

C. Determination of Audit Activities. The City of Sheboygan shall determine the systems or activities that will be tracked or audited by:

1. Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk analysis and ongoing risk management processes (see Risk Analysis and Risk Management Policy and Procedure);

2. Maintaining Confidentiality, Integrity, and Availability of ePHI applications and systems;

3. Assessing the appropriate scope of system audits based on the size and needs of The City of Sheboygan by asking:

   a. What information/ePHI is at risk;

   b. What systems, applications or processes are vulnerable to unauthorized or inappropriate Access;

   c. What activities should be monitored ("C.R.U.D." – Create, Read, Update, Delete); and

   d. What information should be included in the audit record.

4. Assessing available organizational resources.

D. Trigger Events. The City of Sheboygan shall identify "trigger events" or criteria that raise awareness of questionable conditions of viewing of confidential information. The "events" may be applied to The City of Sheboygan as a whole or may be specific to a department, unit, or application. The City of Sheboygan shall provide immediate auditing in response to:

1. A Workforce member complaint;

2. Suspected breach of Confidentiality; and

3. High risk or problem-prone event.

E. Frequency of Audits. The City of Sheboygan shall determine auditing frequency by reviewing past experience, current and projected future needs, and industry trends and events. The City of Sheboygan will determine its ability to generate, review, and respond to audit reports. The City of Sheboygan recognizes that failure to address automatically generated audit logs, trails, and reports through a

systematic review process may be more detrimental to the organization than not auditing at all.

F. **Auditing Tools.** The City of Sheboygan's Security Officer or designee is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Use of such tools is explicitly prohibited by others without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

1. Scanning tools and devices;
2. War dialing software;
3. Password cracking utilities;
4. Network "sniffers"; and
5. Passive and active intrusion detection systems.

G. **Data Elements.** Audit documentation and reporting tools shall address, at a minimum, the following data elements:

1. Application, system, network, department, and/or User audited;
2. Audit type;
3. Person/department responsible for audit;
4. Date(s) of audit;
5. Reporting responsibility/structure for review of audit results;
6. Conclusions;
7. Recommendations;
8. Actions;
9. Assignments; and
10. Follow-up.

H. **Review Process.** The process for review of audit logs, trails, and reports shall include:

1. Description of the activity as well as rationale for performing audit;

2. Identification of which Workforce members or department/unit will be responsible for review (Workforce members shall not review audit logs which pertain to their own system activity);

3. Frequency of the auditing process;

4. Determination of significant events requiring further review and follow-up (see Security Incident Response Policy and Procedure); and

5. Identification of appropriate reporting channels for audit results and required follow-up.

I. Vulnerability Testing. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), check if publicly known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

1. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third-party auditing vendor should not be providing the organization IT oversight services.

2. Testing shall be done on a routine basis. (See System Build/Change Control Policy and Procedure.)

J. Audit Requests for Specific Cause.

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources, including, but not limited to: Human Resources, Risk Management, Privacy Officer, Security Officer and/or a member of The City of Sheboygan's leadership team.

2. A request for an audit for a specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by The City of Sheboygan's Privacy Officer or Security Officer.

3. A request for an audit as a result of an Individual concern shall be initiated by The City of Sheboygan's Privacy Officer and/or Security Officer. Under no circumstances shall detailed audit information be shared with the Individual at any time. The City of Sheboygan is not obligated to provide a detailed listing of those Workforce members Accessing an Individual's PHI (an appropriate operational function).

    a. Should the audit disclose that a Workforce member has Accessed an Individual's PHI inappropriately, the Minimum Necessary/least privileged information shall be shared with The City of Sheboygan's Director of Human Resources and Labor Relations to determine appropriate sanction/corrective disciplinary action.

b. Only De-Identified Health Information shall be shared with the Individual regarding the results of the investigative audit process. This information will be communicated to the Individual by The City of Sheboygan's Privacy Officer or designee. Prior to communicating with the Individual, The City of Sheboygan shall consider whether risk management and/or legal counsel should be consulted.

K. Evaluating and Reporting Audit Findings.

1. Audit information that is routinely gathered must be reviewed in a timely manner by the individual and/or department responsible for the activity/process.

2. The reporting process shall allow for meaningful communication of the audit findings to those departments/units sponsoring the activity.

   a. Significant findings shall be reported immediately in a written format. The City of Sheboygan's Security Incident Report Form may be utilized to report a single event.

   b. Routine findings shall be reported to the sponsoring leadership structure in a written report format.

3. Reports of audit results shall be limited to internal use on a Minimum Necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.

4. Security audits constitute an internal, confidential monitoring practice that may be included in The City of Sheboygan's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits, which may further expose organizational risk, are shared with extreme caution. Generic security audit information may be included in organizational reports (individually identifiable health information shall not be included in the reports).

5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring departments/units.

L. Auditing Access and Activity.

1. Periodic monitoring of vendor information system activity shall be carried out to ensure that Access and activity is appropriate for privileges granted and necessary to the arrangement between The City of Sheboygan and the third party.

2. If it is determined that the vendor has exceeded the scope of Access privileges, The City of Sheboygan's leadership must reassess the business relationship. (See Subcontractor Agreements Policy and Procedure.)

3. If it is determined that a subcontractor has violated the terms of the BAA, The City of Sheboygan must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

M. Audit Log Security Controls and Backup.

1. Audit logs shall be protected from unauthorized Access or modification so the information they contain will be available if needed to evaluate a Security Incident. Generally, system administrators shall not have Access to the audit trails or logs created on their systems.

2. Whenever possible, audit trail information shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent Access to audit trails by those with system administrator privileges. This is done to apply the security principle of "separation of duties" to protect audit trails from hackers. Audit trails maintained on a separate system would not be available to hackers who may break into the network and obtain system administrator privileges. A separate system would allow The City of Sheboygan to detect hacking Security Incidents.

3. Audit logs maintained within an application shall be backed up as part of the application's regular backup procedure.

4. The City of Sheboygan shall audit internal backup, storage, and data recovery processes to ensure that the information is readily available in the manner required. Auditing of data backup processes shall be carried out:

   a. On a periodic basis (recommend at least annually) for established practices and procedures; and

   b. More often for newly developed practices and procedures (e.g., weekly, monthly, or until satisfactory assurance of reliability and Integrity has been established).

N. Workforce Training, Education, Awareness, and Responsibilities. The City of Sheboygan's Workforce members are provided training, education, and awareness on safeguarding the privacy and security of business information and PHI. The City of Sheboygan's commitment to auditing Access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a Workforce member's failure to comply

with The City of Sheboygan's policies and procedures. (See Compliance Training and Education Policy and Procedure and Sanction and Discipline Policy and Procedure.)

O. External Audits of Information Access and Activity. Information system audit information and reports gathered from contracted external audit firms and vendors shall be evaluated and appropriate corrective action steps taken as indicated. Prior to contracting with an external audit firm, The City of Sheboygan shall:

1. Outline the audit responsibility, authority, and accountability;

2. Choose an audit firm that is independent of other organizational operations;

3. Ensure technical competence of the audit firm staff;

4. Require the audit firm's adherence to applicable codes of professional ethics;

5. Obtain a signed HIPAA-compliant subcontractor business associate agreement; and

6. Assign organizational responsibility for supervision of the external audit firm.

References	45 C.F.R. § 164.308(a)(1)(ii)(D) – Information System Activity Review Risk Analysis and Risk Management Policy and Procedure Security Incident Response Policy and Procedure Security Incident Report Form System Build/Change Policy and Procedure Business Associate and Business Associate Agreements Policy and Procedure Compliance Training and Education Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

V. INFORMATION ACCESS MANAGEMENT

1. PURPOSE

To establish procedures for authorizing appropriate Access to The City of Sheboygan's information systems containing ePHI.

2. POLICY

A. The City of Sheboygan's Commitment. Safeguarding Access to ePHI and ePHI systems is integral to The City of Sheboygan's compliance efforts under the Security Rule. The City of Sheboygan does all that is reasonable to protect the Confidentiality, Integrity, and Availability of ePHI by taking reasonable steps to manage Access to ePHI appropriately. In accordance with the Security Rule's requirements, The City of Sheboygan provides Access to ePHI to Workforce members who are properly authorized based on their need to know.

B. Access Management Process. The Access management process includes documenting the granting of Access to The City of Sheboygan's information systems containing ePHI. The process must include:

1. Granting different levels of Access to ePHI based on defined job tasks;

2. Tracking and logging authorization of Access to ePHI; and

3. Regular review and revision, as necessary, of authorization of Access to ePHI.

C. Access Based on Risk Analysis. The type and extent of Access authorized to The City of Sheboygan's information systems containing ePHI will be based upon risk analysis. At a minimum, the risk analysis will consider the following factors:

1. The importance of the applications running on the information system;

2. The value or sensitivity of the PHI on the information system;

3. The extent to which the information system is connected to other information systems; and

4. The need to Access the information on the system.

D. Access Establishment. ePHI Access management includes a documented process of establishing, documenting, reviewing, and modifying Access to The City of Sheboygan's information systems containing PHI.

3. PROCEDURE

A. Access Authorization. Only Workforce members whose job duties require Access to ePHI will be allowed Access by the Security Officer (*See* User Access Tracking

Attachment). No Workforce members may willfully attempt to gain Access to The City of Sheboygan information systems containing ePHI for which they have not been given proper authorization or have no need to know.

B. Authorized Users.

1. Prospective employees of the City of Sheboygan may be subject to a background check. Information that may be obtained or requested includes information relating to references, past employment, work habits, education, judgments, liens, criminal background and offenses, character general reputation, social media presence, and driving records.

2. As a condition of Access to any The City of Sheboygan information system that contains ePHI, Workforce members are required to read, sign, and comply with The City of Sheboygan Confidentiality and Information Access Agreement.

3. Adding new Workforce members to the IT Infrastructure and systems along with other systems necessary to perform their job duties will be completed by the Security Officer.

4. Upon voluntary or involuntary termination, off-boarding, and on or before the exiting Workforce member's last day, the IT Department will be notified of what Access must be disabled.

5. Where appropriate, Users will be supervised by an appropriate The City of Sheboygan employee when Users are Accessing The City of Sheboygan's information systems containing ePHI.

C. Personal Mobile Device Policy

D. Third Parties.

1. Third Party Access. Before third-party persons are granted Access to information systems containing ePHI, a risk analysis will be performed. At a minimum, the risk analysis will consider the following factors:

   a. Type of Access required;

   b. Need for Access;

   c. Sensitivity of the ePHI on the information system;

   d. Security controls on the information system; and

   e. Security controls used by the third party.

2. Agreements with Third Parties. Access by third parties to information systems containing ePHI will be allowed only after an agreement has been signed defining the terms of Access. The agreement will include:

   a. The security process and controls necessary to ensure compliance with The City of Sheboygan's security standards;

   b. Restrictions regarding the Use and Disclosure of The City of Sheboygan's PHI; and

   c. The City of Sheboygan's right to monitor and revoke third party persons' Access and activity.

3. Third Party Supervision. Where appropriate, third parties will be supervised by an appropriate The City of Sheboygan employee when such third parties are Accessing The City of Sheboygan's information systems containing ePHI.

E. Unauthorized Access Not Permitted. Workforce members and third-party Users shall not attempt to gain Access to The City of Sheboygan information systems containing ePHI for which they have not been given proper authorization.

References	45 C.F.R. § 164.308(a)(3)(ii)(A) – Authorization and/or Supervision 45 C.F.R. § 164.308(a)(3)(ii)(B) – Workforce Clearance Procedure 45 C.F.R. § 164.308(a)(4)(i) – Information Access Management 45 C.F.R. § 164.308(a)(4)(ii)(B) – Access Authorization Personal Mobile Device Policy Sanction and Discipline Policy and Procedure
Attachments	User Access Tracking Attachment Confidentiality and Information Access Agreement
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

VI. ACCESS ESTABLISHMENT, MODIFICATION, AND REVIEW

1. PURPOSE

To establish procedures for implementing a process for establishing, documenting, reviewing, and modifying Access to The City of Sheboygan's information systems containing ePHI.

2. POLICY

In accordance with the Security Rule, The City of Sheboygan must have a formal documented process for establishing, documenting, reviewing, and modifying Access to The City of Sheboygan's information systems containing ePHI.

3. PROCEDURE

A. Access Authorization. The City of Sheboygan must have a formal, documented process for establishing, documenting, reviewing, and modifying Access to The City of Sheboygan's information systems containing ePHI. At a minimum, the process must include:

1. The procedure for establishing different levels of Access to The City of Sheboygan's information systems containing ePHI;

2. Procedure for documenting established levels of Access to The City of Sheboygan's information systems containing ePHI;

3. Procedure for regularly reviewing The City of Sheboygan's Workforce member Access privileges to The City of Sheboygan's information systems containing ePHI. Reviews will be accomplished at intervals that meet applicable governing directives; and

4. Procedure for modifying The City of Sheboygan's Workforce member Access privileges to The City of Sheboygan's information systems containing ePHI.

B. Access Establishment.

1. Properly authorized and trained Workforce members may Access The City of Sheboygan's information systems containing ePHI. Such Access will be established via a formal, documented process. At a minimum, this process must include:

   a. Identification and definition of permitted Access methods;

   b. Identification and definition of the length of time that Access will be granted;

c. Procedure for both granting a Workforce member an Access method (e.g., password or token) and changing an existing access method;

d. Procedure for managing Access rights in a distributed and networked environment; and

e. Appropriate tracking and logging of activities by authorized Workforce members of The City of Sheboygan's information systems containing ePHI.

2. Where appropriate, security controls or methods that allow Access to be established to The City of Sheboygan's information systems containing ePHI include, at a minimum:

a. Unique User identifiers (hereinafter "User IDs") that enable individual Users to be uniquely identified.

b. User IDs will not give any indication of the User's privilege level. Common or shared identifiers will not be used to gain access to The City of Sheboygan information systems containing ePHI.

c. When User IDs are insufficient or inappropriate, shared identifiers may be used to gain Access to The City of Sheboygan's information systems not containing ePHI. However, this should be a last resort when there are no other feasible alternatives.

d. Further, any time shared identifiers are used, the system and/or applicable administrators and data owners must have a mechanism of tracking the individuals that are aware of the shared identifiers/credentials. The shared identifiers/credentials must be changed promptly any time an individual with knowledge of the credentials and passphrase transfers or is terminated from employment or no longer needs Access to the ePHI for any reason.

e. The prompt removal or disabling of Access methods for persons and entities that no longer need access to The City of Sheboygan's information systems ePHI.

f. Verification that redundant User IDs are not issued.

3. Access to The City of Sheboygan's information systems containing ePHI must be limited to Workforce members who need Access to specific ePHI in order to perform their job responsibilities.

4. Administrator passwords will be stored in a secure location in case of an emergency or disaster.

C. **Review of Access Rights.** The Security Officer, appropriate The City of Sheboygan information system supervisors, or their designated delegates must regularly review Workforce member Access rights to The City of Sheboygan's information systems containing ePHI to ensure that they are provided only to those who have a need for specific ePHI in order to accomplish a legitimate task. Such rights must be revised as necessary. Reviews should be accomplished at intervals that meet applicable governing directives.

D. **Tracking User Access.** Access by The City of Sheboygan's Workforce members must be tracked and logged. At a minimum, such tracking and logging must provide the following information:

1. Date and time of Access;

2. Identification of the Workforce member who Accessed data; and

3. Identification of data records Accessed by Workforce member.

This information must be securely maintained.

E. **Tracking User Access Revision.** All revisions to The City of Sheboygan's Workforce member Access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information:

1. Date and time of Access revision;

2. Identification of the Workforce member whose Access is being revised;

3. Brief description of revised Access right(s); and

4. Reason for revision.

5. This information must be securely maintained.

References	45 C.F.R. § 164.308(a)(4)(ii)(C) – Access Establishment and Modification Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

VII. PROTECTION FROM MALICIOUS SOFTWARE

1. PURPOSE

To establish procedures to train and remind Workforce members about The City of Sheboygan's process of guarding, detecting, and reporting malicious software that poses a risk to its information systems.

2. POLICY

The City of Sheboygan will provide procedures as well as regular training and awareness to its Workforce members about its process of guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.

3. PROCEDURE

A. Malicious Software Protection Program. The City of Sheboygan should be able to detect and prevent malicious software, particularly viruses, worms, and malicious code. The malicious software prevention, detection, and reporting process includes:

1. Installation and regular updating of anti-virus software;

2. Examination of data on electronic media and data received over networks to ensure that it does not contain malicious software;

3. The examination of electronic mail attachments and data downloads for malicious software;

4. Reporting of suspected or known malicious software by Workforce members;

5. Verification that all information relating to malicious software is accurate and informative;

6. Inclusion of a provision in The City of Sheboygan's policies that Workforce members will not modify web browser security settings without appropriate authorization; and

7. Inclusion of a provision in The City of Sheboygan's policies that unauthorized software will not be installed on The City of Sheboygan's information system and devices.

B. Malicious Software Training. The City of Sheboygan's malicious software training and awareness covers topics including, but not limited to:

1. How to identify malicious software;

2. How to report malicious software;

3. How to effectively use anti-virus software;

4. How to avoid downloading or receiving malicious software; and

5. How to identify malicious software hoaxes.

C. Disabling Protections Not Permitted. Unless appropriately authorized, it is the policy of The City of Sheboygan that Workforce members shall not bypass or disable anti-virus software.

D. Documentation. The City of Sheboygan shall maintain documentation of malicious software training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(5)(ii)(B) – Protection from Malicious Software Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

VIII. LOG-IN MONITORING

1. PURPOSE

To establish procedures to monitor, train, and remind Workforce members about The City of Sheboygan's process of monitoring log-in attempts and reporting discrepancies.

2. POLICY

The City of Sheboygan will provide regular monitoring as well as training and awareness to its Workforce members about its process of monitoring log-in attempts and reporting discrepancies**.**

See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.

3. PROCEDURE

A. Secure Log-in Process. Access to all THE CITY OF SHEBOYGAN information systems is via a secure log-in process. The process:

1. Does not display information system or application identifying information until the log-in process has been successfully completed;

2. Validates log-in information only when all the data input has been done; and

3. Limits the number of unsuccessful log-in attempts to no more than five (5) consecutive attempts before requiring a time-out and/or challenge requirement for resetting the log-in.

B. Log-in Process Abilities. Log-in process includes the ability to:

1. Record unsuccessful log-in attempts, including the following information:

   a. IP address of the failed log-in;

   b. Log-in "username" used when log-in was unsuccessful.

2. Limit the maximum number of attempts allowed for the log-in procedure to five (5) attempts before the username needs to be reset by the administrator.

C. Log-in Training. Log-in monitoring training and awareness covers topics including, but not limited to:

1. How to effectively use secure log-in process;

2. How to detect log-in discrepancies; and

3. How to report log-in discrepancies.

D. Documentation. The City of Sheboygan shall maintain documentation of log-in training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308 (a)(5)(ii)(C) Log-in Monitoring Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

IX. PASSWORD MANAGEMENT

1. PURPOSE

To establish procedures to manage as well as provide regular training and awareness to Workforce members about creating, changing, and safeguarding passwords.

2. POLICY

The City of Sheboygan will maintain as well as provide regular training and awareness to Workforce members about creating, changing, and safeguarding passwords.

See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.

3. PROCEDURE

A. Password Management System Requirements. The City of Sheboygan's password management system:

1. Requires use of individual passwords to maintain accountability.

2. Where appropriate, allows Workforce members and authorized Users from external organizations to select and change their own passwords.

3. Requires unique passwords as per the standards defined by The City of Sheboygan.

4. Does not display passwords in clear text when they are being input into an application.

5. Requires the storage of passwords in encrypted form using a one-way encryption algorithm.

6. Requires initial password(s) issued to new Workforce members to be valid only for the new User's first log-in to a Workstation. At initial log-in, the User must be required to choose another password.

7. Requires the changing of default vendor passwords following installation of software.

8. Prompts Users every 90 days to change the password.

9. Requires removing access to credentials as soon as possible but no later than 24 hours after a User's Access has been terminated.

B. Password Creation Standards. The password creation standard requires:

1. The password must be at least 10 characters long;

2. The password must be strong (preferred to include at least one capital letter, one number, and one character).

C. Password Management and Training.

1. The Security Officer is responsible for training all Users in relation to password use and management.

2. Password management training and awareness involves requirements for use of information systems, including, but not limited to:

   a. Passwords should not be shared or given to someone else to use;

   b. Passwords should not be displayed in a publicly accessible location (i.e., no post-it notes on the computer);

   c. Workforce members should make a reasonable effort to ensure that password entry is not observed (i.e., do not log in while others are in your area);

   d. Passwords should be changed whenever there is any indication of possible information system or password compromise;

   e. Temporary passwords should be changed in the first log-in;

   f. Workforce members should not use the "remember password" feature;

   g. Workforce members are discouraged from using the same password for personal and business use;

   h. Workforce members are discouraged from using the same password for various Access needs when possible;

   i. Data entry should not take place under another Workforce member's password;

   j. All Workforce members should understand that all activities involving their User identification and password will be attributed to them; and

   k. Workforce members will immediately report (if known) a compromised password(s) to the Security Officer. Passwords that are identified as compromised will be replaced or terminated within one business day.

D. Documentation. The City of Sheboygan shall maintain documentation of password management training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(5)(ii)(D) – Security Awareness and Training; Password Management Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

X. CONTINGENCY PLANNING & RECOVERY STRATEGY

1. PURPOSE

To establish procedures to effectively prepare and respond to emergencies or disasters in order to protect the Confidentiality, Integrity, and Availability of ePHI and The City of Sheboygan's information systems.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to effectively prepare for and respond to emergencies or disasters in order to protect the Confidentiality, Integrity, and Availability of ePHI and The City of Sheboygan's information systems.

B. Emergency Response Process. The City of Sheboygan will have a formal process to prepare for and effectively respond to emergencies and disasters that may damage the Confidentiality, Integrity, or Availability of PHI or The City of Sheboygan's information systems that includes but is not limited to:

1. Regular analysis of the criticality of information systems;

2. Development and documentation of a disaster and emergency recovery strategy consistent with business objectives and priorities;

3. Development and documentation of a disaster recovery plan that is in accordance with the above strategy;

4. Development and documentation of an emergency mode operations plan that is in accordance with the above strategy; and

5. Regular testing and updating of the disaster recovery and emergency mode operations plans.

C. System Controls. The disaster and emergency response process is intended to reduce the disruption to The City of Sheboygan's information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes identify and reduce risks to information systems, limit damage caused by disasters and emergencies, and ensure the timely resumption of significant information systems and processes. Such controls and processes are proportionate with the value of the information systems being protected or recovered.

3. PROCEDURE

A. Environmental Controls.

1. The Security Officer:

a. Makes all reasonable efforts to have security controls and contingency plans in place that minimize the amount of time systems may be down to the least possible, but no more than 72 hours for critical systems, as long as it does not unduly hinder operational performance, jeopardize security, or increase costs.

b. Obtains, reviews, approves, and maintains documentation of facility security, environmental controls, and contingency plans (including testing done).

2. Critical ePHI systems are on an uninterruptible power supply with warning lights or alarms and a generator. The generator is tested weekly. The equipment contains sensors to alert of possible outages. The generator powers this equipment upon power loss.

3. The server room contains the following:

a. A cooling system;

b. Fire suppression system;

c. Electrical fire rated fire extinguisher;

d. Temperature and fire alarms/paging and generator paging;

e. Locked room with access limited to minimum necessary needed to maintain/recover systems; and

4. The City of Sheboygan's vendors that maintain, store, and/or back up ePHI on behalf of The City of Sheboygan are required to have the above-stated controls in place at a minimum. Exceptions are approved and documented by the Security Officer.

B. **Facility Security.** Only the following individuals (who are able to assist in restoring Access to ePHI) may have access to and be in the server room as well as have access to backups, even during emergencies and disaster situations: Facilities Director. (See Facility Access Controls: Security Plan Policy and Procedure.)

C. **Contingency Plan.** The Security Officer oversees and has the authority and overall responsibility for facilitating the implementation, activation, coordination, and documentation of a contingency plan and disaster recovery operations, including the following:

1. Maintains a contact list for each key system with the current contingency plan/disaster recovery plan. The contact list includes key Workforce members, key vendors, and other individuals that help support and recover systems (e.g., telecommunications/phone, ISPs, etc.).

2. Maintains an inventory asset list for each system, application, server, hardware, IS equipment (Workstations, portable devices, etc.), network information specifications, etc. purchased by or leased by The City of Sheboygan that are used to Access, create, receive, maintain, or transmit ePHI. This list includes, at a minimum and as applicable:

    a. Critical functions that help determine how important each system is to business needs;

    b. Indication of the critical systems that are supported at alternate sites;

    c. Location and who uses each ePHI system, Workstation, and portable device;

    d. Model and serial numbers, manufacturer, operating systems, warranty information, etc. so items can easily be replaced, as applicable;

    e. Interdependencies/interoperability on other systems, applications, servers, etc., with a recovery plan for each;

    f. Expected date of retirement; and

    g. Retired assets.

3. Assigns a data criticality level for each system, application, server, hardware, IS equipment, network information/specifications, etc. (See Information Classification Table and Information Classification Questionnaire in Risk Analysis and Risk Management Policy and Procedure.) All software applications and data points that create, receive, maintain, or transmit ePHI are included on the list. Applications, systems, and/or networks that need to be available at all times and need to be recovered/restored first are prioritized.

4. Maintains a current network diagram of all servers, systems, interfaces, etc.

D. Emergency Response Training. The City of Sheboygan's Workforce members receive regular training and awareness on disaster preparedness and disaster and emergency response processes. (See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.)

E. Documentation. The City of Sheboygan shall maintain documentation of its contingency plan consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(7) – Contingency Plan 45 C.F.R. § 164.310(a)(2)(i) – Facility Access Controls/Contingency Operations 45 C.F.R. § 164.310(a)(2)(ii) – Access Control/Emergency Access Procedure Risk Analysis and Risk Management Policy and Procedure Facility Access Controls: Security Plan Policy and Procedure

	Compliance Training and Education Policy and Procedure Facility Access Controls: Contingency Operations Policy and Procedure Retention of HIPAA Documentation Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XI. CONTINGENCY PLAN: DATA BACKUP PLAN

1. PURPOSE

To establish procedures to regularly back up and securely store all ePHI on The City of Sheboygan's information systems and regularly test the backup and restoration procedures.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to back up and securely store all ePHI on its information systems and electronic media. The City of Sheboygan will have formal, documented procedures for creating and maintaining retrievable exact copies of ePHI. At a minimum these procedures must:

1. Identify the computing systems to be backed up;

2. Provide a backup schedule;

3. Identify where backup media are stored and who may Access them; and

4. Outline the restoration process and identify who is responsible for ensuring the backup of the ePHI.

B. Frequency, Retention, and Storage of Backups. The criticality of the data will determine the frequency of data backups, retention of data backups, as well as where data backups and restoration procedures will be stored.

C. Storage of Backups. Backup copies of ePHI will be stored at a secure location and must be accessible to authorized Workforce members for prompt retrieval of the information. The secure location must be as geographically distant from the location of The City of Sheboygan's computing system as is feasible.

D. Restoration Procedures. Restoration procedures for ePHI must be regularly tested to ensure that they are effective and that they can be completed within the time allotted in the disaster recovery plan.

References	45 C.F.R. § 164.308(a)(7)(ii)(A) – Data Backup Plan Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XII. CONTINGENCY PLAN: EMERGENCY MODE OPERATIONS PLAN

1. PURPOSE

To establish procedures for an emergency mode operations plan to enable the continuation of crucial business processes that protect the security of The City of Sheboygan's information systems containing ePHI during and immediately after a crisis situation.

2. POLICY

A. **The City of Sheboygan's Commitment.** The City of Sheboygan commits to have an emergency mode operations plan for protecting its information systems containing ePHI during and immediately after a crisis situation.

B. **Minimum Elements.** The City of Sheboygan will have a formal, documented emergency mode operations plan for protecting its information systems containing ePHI during and immediately after a crisis situation. At a minimum, the plan must:

1. Identify and prioritize emergencies that may impact The City of Sheboygan's information systems containing ePHI;

2. Define procedures for responding to specific emergencies that impact information systems containing ePHI;

3. Define procedures for a crisis situation, during and immediately after, that will maintain the processes and controls that ensure the Confidentiality, Integrity, and Availability of ePHI; and

4. Define a procedure that ensures that authorized employees can enter The City of Sheboygan's facilities to enable continuation of processes and controls that protect ePHI while The City of Sheboygan is operating in emergency mode.

C. **Workforce Training.** All Workforce members must receive annual training and awareness on the emergency mode operations plan. All appropriate Workforce members will have access to a current copy of the plan.

3. PROCEDURE

A. Individuals with hard-key access to the server room building: Facilities Director.

B. Individuals with hard-key access to the server room: Facilities Director.

C. In the event of a power failure, The City of Sheboygan may close if the backup generator is not functional and The City of Sheboygan is unable to continue daily operations. The decision will be based on the severity and expected length of the power outage. A final determination will be made by the Security Officer or a member of the HIPAA Security Team if the Security Officer is not available.

D. Security Officer will check inventory of operating systems after the emergency as necessary to assess damage.

E. If necessary, The City of Sheboygan will operate systems offsite until the emergency/occurrence is resolved.

F. In the event of an emergency, The City of Sheboygan will make every attempt to make certain that all PHI is kept confidential.

G. **Documentation.** The City of Sheboygan shall maintain documentation of emergency mode operations plan training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(7)(ii)(C) – Emergency Mode Operation Plan Sanction and Discipline Policy and Procedure Retention of HIPAA Documentation Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, Privacy Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XIII. CONTINGENCY PLAN: TESTING AND REVISION PROCEDURES

1. PURPOSE

To establish procedures for conducting regular testing of information technology disaster recovery and emergency mode operations plans to ensure that they are up to date and effective.

2. POLICY

A. **The City of Sheboygan's Commitment.** The City of Sheboygan commits to regularly test its information technology disaster recovery and emergency mode operations plans.

B. **Regular Testing.** The City of Sheboygan will conduct regular testing of its disaster recovery and emergency mode operation plans to ensure they are current and operative. Criticality of data and resource availability will determine the frequency of testing. Testing will be conducted on an annual basis or as frequently as is feasible.

C. **Result Documentation.** The results of these tests will be formally documented. The disaster recovery and emergency mode operations plans will be revised as necessary to address issues or gaps identified in the testing process.

3. PROCEDURE

A. **Frequency and Drills.** Contingency plan testing is done on an annual basis at a minimum. A scenario-based walk-through or mock drill is done to examine the plans and determine the need for changes.

B. **Component Failure.** During the normal use of any system, components fail. The Security Officer will document why the system was down and how the system was recovered. The Security Officer will maintain this documentation as part of the contingency plan testing files.

C. **Maintenance and Revision of Plan.** The Security Officer is responsible for maintenance and revision of the contingency plans/disaster response plan, which shall be reviewed and revised on an annual basis, after each disaster incident (whether a planned drill or actual disaster), and when needed to ensure that the information it contains is current.

D. **Documentation.** The City of Sheboygan shall maintain documentation created pursuant to this Policy consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(7)(ii)(D) – Testing and Revision Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XIV. CONTINGENCY PLAN: APPLICATION AND DATA CRITICALITY ANALYSIS

1. PURPOSE

To establish procedures for defining and identifying the criticality of information systems and the data contained within them.

2. POLICY

The City of Sheboygan commits to conduct an annual analysis of the criticality of its information systems. The prioritization of information systems will be based on an analysis of the impact to The City of Sheboygan's services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time.

3. PROCEDURE

A. Minimum Elements. The City of Sheboygan will have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them. At a minimum, the process will include:

1. Creating an inventory of interdependent systems and their dependencies;
2. Documenting the criticality of information systems;
3. Identifying and documenting the impact to The City of Sheboygan's services;
4. Identifying the maximum time periods that health care computing systems can be unavailable; and
5. Prioritizing health care computing systems components according to their criticality to The City of Sheboygan's ability to function at normal levels.

B. Frequency. The criticality analysis will be conducted at regular intervals, at least annually.

C. Documentation. The City of Sheboygan shall maintain documentation created pursuant to this Policy consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(7)(ii)(E) – Applications and data criticality analysis Retention of HIPAA Documentation Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XV. PERIODIC EVALUATION OF STANDARDS

1. PURPOSE

To establish procedures to perform a technical and nontechnical evaluation, based upon the standards implemented under the Security Rule and, subsequently, in response to environmental or operational changes affecting the security of ePHI, that will help to establish the extent to which The City of Sheboygan's HIPAA Policies and Procedures Manual meets the requirements of the Security Rule.

2. POLICY

The City of Sheboygan commits to perform technical and nontechnical evaluation of implemented standards to determine the level of compliance with the Security Rule.

3. PROCEDURE

A. Evaluation. The evaluation will include but not be limited to:

1. Penetration analysis;

2. Password integrity; and

3. Compliance.

The evaluation will include review of pertinent records, including any Security Incidents and/or Breaches, The City of Sheboygan's HIPAA Policies and Procedures Manual, direct observation of workplace practices, and observation of compliance with The City of Sheboygan's HIPAA Policies and Procedures Manual.

B. Performance of Evaluation. Designated Workforce members and the Security Officer will perform the review of technical and nontechnical Safeguards.

C. Review of The City of Sheboygan's HIPAA Policies and Procedures Manual. The Security Officer, with assistance from the Privacy Officer, as appropriate, will review The City of Sheboygan's HIPAA Policies and Procedures Manual: (i) at least on an annual basis in order to ensure that it is current or (ii) more frequently as appropriate or in case of Breach response. The City of Sheboygan's HIPAA Policies and Procedures Manual will be evaluated and edited as needed. Documentation of such evaluation will be maintained by the Security Officer and Privacy Officer.

D. Documentation. The City of Sheboygan shall maintain documentation created pursuant to this Policy consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(8) – Evaluation Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XVI. FACILITY ACCESS CONTROLS: CONTINGENCY OPERATIONS

1. PURPOSE

To establish procedures for The City of Sheboygan facility access in support of restoration of lost data under the Contingency Plan: Disaster Recovery Plan Policy and Procedure and Contingency Plan: Emergency Mode Operations Plan Policy and Procedure in the event of an emergency.

2. POLICY

The City of Sheboygan commits to ensure that, in the event of a disaster or emergency, appropriate Workforce members are able to enter its facilities to take necessary actions as defined in The City of Sheboygan's disaster recovery plan and emergency mode operations plan.

3. PROCEDURE

A. Safeguards. The City of Sheboygan will implement the following Safeguards:

1. The City of Sheboygan will ensure that in the event of a disaster or emergency, appropriate Workforce members can enter the facility to take necessary actions defined in its Contingency Plan: Disaster Recovery Plan Policy and Procedure and Contingency Plan: Emergency Mode Operations Plan Policy and Procedure.

2. Based on its disaster recovery plan and emergency mode operations plan, The City of Sheboygan will develop, implement, and regularly review a formal, documented procedure that ensures that authorized employees can enter The City of Sheboygan's facilities to enable continuation of processes and controls that protect ePHI while The City of Sheboygan is operating in emergency mode.

3. In the event of an emergency, only authorized Workforce members may administer or modify processes and controls that protect ePHI contained on information systems. Such Workforce members or roles will be defined in the Contingency Plan: Disaster Recovery Plan Policy and Procedure and Contingency Plan: Emergency Mode Operations Plan Policy and Procedure.

References	45 C.F.R. § 164.310(a)(2)(i) – Contingency Operations Contingency Plan: Disaster Recovery Plan Policy and Procedure Contingency Plan: Emergency Mode Operations Plan Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XVII. FACILITY ACCESS CONTROLS: SECURITY PLAN

1. PURPOSE

To establish procedures to safeguard The City of Sheboygan's facilities and the equipment therein from unauthorized physical Access, tampering, and theft.

2. DEFINITIONS

"Access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

3. POLICY

The City of Sheboygan commits to maintaining a facility security plan for protecting its facilities and the equipment contained therein. The City of Sheboygan will make a reasonable effort to limit physical Access, tampering, and theft.

4. PROCEDURE

A. Maintenance and Review of Plan. The City of Sheboygan will maintain and review annually a formal, documented facility security plan that describes how its facilities and equipment within them will be appropriately protected. The plan will be revised as necessary.

B. Minimum Elements. At a minimum, The City of Sheboygan's facility security plan will address the following:

1. Identification of computing systems to be protected from unauthorized physical Access, tampering, and theft;

2. Identification of processes and controls used to protect computing systems from unauthorized physical Access, tampering, and theft;

3. Actions to be taken if unauthorized physical Access, tampering, or theft attempts are detected/made against computing systems; and

4. A maintenance schedule which will specify how and when the plan will be tested, as well as the process for maintaining the plan.

C. Workforce Responsibility.

1. Workforce members will take necessary steps to protect and secure PHI in their areas.

2. To minimize unauthorized Access to computing systems containing ePHI, Workforce members will refrain, to the extent possible, from accessing areas to which they do not have authorized accessibility.

3. Workforce members will immediately report the entrance of another Workforce member present in a non-assigned work area to their supervisor, Privacy Officer, or Security Officer.

D. Routine Repairs and Maintenance. All routine repairs and maintenance will be done during business hours with appropriate Workforce members available to oversee and ensure that inappropriate Access and actions are not taken.

E. Documentation. The City of Sheboygan shall maintain documentation of its facility security plan consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(a)(2)(ii) – Facility Security Plan Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XVIII. FACILITY ACCESS CONTROLS: ACCESS CONTROL AND VALIDATION

1. PURPOSE

To establish procedures to control and validate a person's access to The City of Sheboygan facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.

2. POLICY

The City of Sheboygan ensures that approved access shall be limited to Workforce members who have a need for specific physical access in order to accomplish a legitimate task.

3. PROCEDURE

A. Safeguards. The City of Sheboygan will implement the following Safeguards:

1. The City of Sheboygan will identify and document all organizational or functional areas considered sensitive due to the nature of the ePHI that is stored or available within them.

2. After documenting sensitive areas, access rights to such areas will be given only to Workforce members who have a need for specific physical Access in order to accomplish a legitimate task.

3. Keys or access cards will only be distributed to authorized personnel and will be approved prior to release of keys/cards.

4. Physical Access to areas containing ePHI will be approved by the Security Officer or designee.

5. All visitors to sensitive facilities where computing systems are located must show proper identification, provide reason for need to access, and sign in prior to gaining access.

6. Workforce members will immediately report to appropriate management the loss or theft of any device (e.g., card or token) that enables them to gain physical Access to such sensitive facilities.

7. Workforce members will wear an identification badge when inside facilities where computing systems are located and will be encouraged to report unknown persons not wearing such identification.

8. All access rights to The City of Sheboygan's facilities where computing systems are located or software programs that can access computing systems will be reviewed annually and revised as necessary.

References	45 C.F.R. § 164.310(a)(2)(iii) – Access Control and Validation Procedures Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XIX. FACILITY ACCESS CONTROLS: MAINTENANCE RECORDS

1. PURPOSE

To establish policies and procedures to document repairs and modifications to the physical components of a facility that are related to security, e.g. hardware, walls, doors, etc.

2. POLICY

The City of Sheboygan commits to document all repairs and modifications to the physical components of its facilities that are related to the protection of ePHI.

3. PROCEDURE

A. Safeguards. The City of Sheboygan will implement the following Safeguards:

1. The City of Sheboygan will document all repairs and modifications to the physical components of its facilities where computing systems are located. Physical components include, but are not limited to, electronic card access systems, locks, doors, and walls.

2. The City of Sheboygan will conduct an inventory of all the physical components of its facilities that are related to the protection of computing systems on an annual basis, at a minimum. Inventory results will be documented and stored in a secure manner.

3. Repairs or modifications to any physical component listed in the above inventory will be documented. At a minimum, the documentation will include:

    a. Date and time of repair or modification;

    b. Reason for repair or modification;

    c. Person(s) performing the repair or modification; and

    d. Outcome of repair or modification.

References	45 C.F.R. § 164.310(a)(2)(iv) – Maintenance Records Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XX. COMPUTER TERMINALS/WORKSTATIONS

1. PURPOSE

To establish rules for securing computer terminals/Workstations that Access ePHI. Since ePHI can be portable, this Policy requires Workforce members to protect ePHI at The City of Sheboygan's facilities and all other locations.

2. POLICY

Computer terminals and Workstations will be positioned/shielded to ensure that PHI is protected from (a) public view, (b) view by those who do not need to know, whether inadvertently or otherwise, or (c) unauthorized Access.

3. PROCEDURE

A. Positioning of Terminals/Workstations. Computer terminals/Workstations shall be positioned or shielded so that screens are not visible to the public and/or to unauthorized staff. View-limiting screens should be installed where necessary to limit visibility of the screen.

B. Access to Terminals/Workstations. Authorized personnel are granted Access to ePHI. This Access should be limited to specific, defined, documented, and approved applications and level of Access rights.

C. Leaving Workstations/Terminals Unattended.

1. A User may not leave his/her Workstation or terminal unattended for long periods of time (e.g., breaks, lunch, meetings, etc.) without clearing the terminal screen/locking the screen/logging off from the system.

2. Each User is required to log off from the system at the end of his/her work shift.

3. Each User is required to lock his/her computer when it is left unattended for any period of time.

4. Users may not change the automatic inactivity locks on their Workstation.

5. Users are required to ensure that all confidential information in their Workstations is not viewable or accessible by unauthorized persons.

6. When working from home or other non-office work sites, a User is required to protect ePHI from unauthorized Access or viewing.

D. Clearing Screens. A User must clear the terminal screen if the Workstation or terminal is left briefly unattended.

E. **Hard Copies of Data**. Hard copy printed information shall be stored in such a manner that it cannot be viewed or read by the public and/or any unauthorized staff. It must be placed in designated secure areas upon leaving the work area and at the end of the work shift.

F. **Password Sharing.** A User should not:

1. Share or disclose his/her password or User ID with other Workforce members or other non-Workforce members; or

2. Allow Workforce members or other non-Workforce members Access privileges (e.g., piggyback Access) while the User is logged onto the information system used by The City of Sheboygan.

(See Password Management Policy and Procedure.)

G. **IT Support.** When installing new Workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 15 minutes. (See Automatic Logoff Policy and Procedure.)

H. **Training.** The City of Sheboygan will train Workforce members on computer terminals/Workstation obligations. (See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.)

I. **Documentation.** The City of Sheboygan shall maintain documentation of computer terminals/Workstation obligations training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.312(a)(2)(iii) – Automatic Logoff 45 C.F.R. § 164.308(a)(5)(ii)(D) – Security Awareness and Training; Password Management 45 C.F.R. § 164.530 – Administrative Requirements Password Management Policy and Procedure Automatic Logoff Policy and Procedure Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXI. WORKSTATION USE

1. PURPOSE

To establish procedures that specify the proper guidelines to be followed by Workforce members while Accessing information systems containing ePHI and allowable physical attributes of the surroundings of Workstations that have Access to ePHI.

2. POLICY

The City of Sheboygan commits to identify acceptable use of information systems and the proper method of logging into and off the system.

3. PROCEDURE

A. Workforce Responsibility.

1. Workforce members will log off the applications on their Workstations and shut down their computers at the end of their workday. (See Automatic Logoff Policy and Procedure.)

2. For all computers in an active directory when left unattended, a password-protected screensaver will be activated after 15 minutes of non-use. (See Automatic Logoff Policy and Procedure.)

3. Doors leading into offices with desktop/laptops should always be locked when vacated. If the desktop/laptop is in a public area and cannot be secured by a locked door, other security mechanisms must be in place such as security locking cables or cages.

4. If passwords are written down by Users, they are to be kept in a secure location without any indication as to what the password belongs to. No passwords can be kept on post-it notes left around Workstations where anyone can view credentials. (See Password Management Policy and Procedure.)

5. With the exception of IT or other designated staff for auditing or trouble-shooting purposes, Workstations with multiple Users are to be logged off when someone else needs to use the Workstation or if it is no longer in use.

6. Any usage of a Workstation under someone else's log-in credentials will be a violation of this Policy. IT and/or their designee are to only use a Workstation under someone else's log-in for appropriate IT-related functions, such as trouble-shooting, virus removal, etc., and must have the written or verbal approval of the logged-in User. IT and their designee(s) should avoid this when possible. (See Unique User Identification Policy and Procedure.)

B. **Training.** The City of Sheboygan will train Workforce members on Workstation use. (See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.)

C. **Documentation.** The City of Sheboygan shall maintain documentation of Workstation use training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(b) – Workstation Use Automatic Logoff Policy and Procedure Password Management Policy and Procedure Unique User Identification Policy and Procedure Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXII. WORKSTATION SECURITY

1. PURPOSE

To establish procedures to implement Physical Safeguards for all Workstations that Access ePHI and restrict Access to authorized Users.

2. POLICY

The City of Sheboygan commits to protection of Workstations that store or Access ePHI while ensuring that authorized Workforce members have appropriate Access.

3. PROCEDURE

A. Safeguards. The City of Sheboygan will implement the following Safeguards:

1. The City of Sheboygan will prevent unauthorized physical Access to Workstations that can Access ePHI and ensure that authorized Workforce members have appropriate Access.

2. Access to all The City of Sheboygan's Workstations will be authenticated via a process that includes, at a minimum:

    a. User IDs that enable Users to be identified and tracked (see Unique User Identification Policy and Procedure);

    b. Passwords must be masked, suppressed, or otherwise obscured so that unauthorized persons are not able to observe them (see Password Management Policy and Procedure);

    c. The initial password(s) issued to a new Workforce member will be valid only for the new User's first log-in to a Workstation. At initial log-in, the User must be required to choose another password (see Password Management Policy and Procedure); and

    d. Upon termination of Workforce member's employment or contracted services, Workstation Access privileges will be removed within 24 hours. (See Access Establishment, Modification, and Review Policy and Procedure.)

3. Anti-virus software will be installed on Workstations to prevent transmission of malicious software. Such software will be regularly updated.

4. Special precautions will be taken with portable Workstations such as laptops and personal digital assistants (PDA). At a minimum, the following guidelines will be followed with such systems: Update consistent with your standards.

a. ePHI will not be stored on portable Workstations unless such information is appropriately protected through encryption. If ePHI is stored on the portable device, it must be encrypted (see Encryption and Decryption Policy and Procedure);

b. Locking software for unattended laptops will be activated; and

c. Portable Workstations containing ePHI will be carried as carry-on (hand) baggage when Workforce members use public transport such as air travel, subway, etc. They should be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile).

5. For Workstations with ePHI stored locally on hard drives or other memory devices, additional security measures are required. At a minimum these requirements will include:

a. Approval from the Security Officer will be acquired prior to storing ePHI on Workstations or devices external to the existing The City of Sheboygan computer systems. The City of Sheboygan will contact the Security Officer to identify any database or application that will store ePHI. The Security Officer will determine if the application or database is legitimate or if it is a duplicate system. If approval is granted, the Security Officer will review the security controls against the Security Rule requirements;

b. Inventory and documentation of ePHI stored on Workstations is done when Workstations are first installed and will be done at least on an annual basis thereafter;

c. Security Safeguards related to the protection of ePHI stored on Workforce member Workstations will be reviewed and documented; and

d. Data files containing ePHI will be encrypted wherever possible and password-protected.

B. Wireless Access.

1. For purposes of this Policy, wireless devices include all wireless data communication devices connected to any of The City of Sheboygan's internal/external networks. This Policy does not apply to any wireless devices not connecting to The City of Sheboygan's internal/external networks.

2. Access to The City of Sheboygan's network via unsecured wireless communication mechanisms is prohibited.

3. Wireless access passwords will be controlled and issued by the Security Officer.

4. Wireless access passwords will be changed at the discretion of the Security Officer.

C. Workforce Responsibility.

1. All Workforce members who use The City of Sheboygan Workstations will take all reasonable precautions to protect the Confidentiality, Integrity, and Availability of ePHI contained on or Accessed by the Workstations. For example, Workforce members shall position monitors or shield Workstations so that data shown on the screen is not visible to unauthorized persons. (See Computer Terminals/Workstations Policy and Procedure.)

2. Unauthorized Workforce members must not willfully attempt to gain physical Access to Workstations that store or Access ePHI. (See Information Access Management Policy and Procedure.)

3. Workforce members will report loss or theft of any access device (such as a card or token) that allows them physical Access to areas having Workstations that can Access ePHI. (See Facility Access Controls: Access Control and Validation Policy and Procedure.)

4. Workforce members will not share their User accounts or passwords with others. If a Workforce member believes that someone else is inappropriately using a User account or password, he/she must immediately notify the Security Officer. (See Password Management Policy and Procedure.)

5. Workforce members will report theft of all devices to the Privacy Officer and/or Security Officer immediately. (See Facility Access Controls: Security Plan.)

D. Training. The City of Sheboygan will train Workforce members on Workstation security. (See Compliance Training and Education Policy and Procedure for The City of Sheboygan's HIPAA training program, generally.)

E. Documentation. The City of Sheboygan shall maintain documentation of Workstation security training consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(c) – Workstation Security Unique User Identification Policy and Procedure Password Management Policy and Procedure Access Establishment, Modification, and Review Policy and Procedure Encryption and Decryption Policy and Procedure Computer Terminals/Workstations Policy and Procedure Information Access Management Policy and Procedure

	Facility Access Controls: Access Control and Validation Policy and Procedure Facility Access Controls: Security Plan Policy and Procedure Compliance Training and Education Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXIII. DEVICE AND MEDIA CONTROLS: DISPOSAL

1. PURPOSE

To establish procedures for final disposition of ePHI and/or the hardware or electronic media on which it is stored.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to appropriately dispose of information systems and their associated electronic media containing ePHI when they are no longer needed to ensure the security and privacy of the content of the electronic media. All The City of Sheboygan computing systems and associated electronic media containing ePHI must be disposed of properly when no longer needed for legitimate use.

B. Applicability. Information systems and electronic media to which this Policy applies include, but are not limited to, desktops, laptops, personal digital assistants (PDAs), tablets, The City of Sheboygan-issued cell phones, hard disks, SAN disks, SD and similar cards, floppy disks, backup tapes, CD\DVD-ROMs, zip drives, portable hard drives, and flash memory devices (thumb drives).

3. PROCEDURE

A. Preparation for Disposal.

1. Any disposal of inventory containing ePHI must be reported to and approved by the Security Officer or designee for inventory control.

    a. The Security Officer, with assistance of the IT Department removes all software licenses prior to destruction/disposal/sanitization;

    b. Media containing ePHI scheduled for disposal is secured to prevent unauthorized or inappropriate Access until the destruction/disposal/sanitization is complete; and

    c. The Security Officer or designee updates the status of the inventory list, including hardware and licensed software.

B. Methods of Disposal.

1. Data Sanitization. For the disposal of an information system or electronic medium containing ePHI, the data must be completely removed with data sanitization tool(s) that erase or overwrite media in a manner that prevents the data from being recovered consistent with: (i) the methods and procedure outlined in the Destruction/Disposal of PHI Policy and Procedure and (ii) NIST Special Publication 800-88 – Guidelines for Media

Sanitization. "Deleting" typically does not destroy data and may enable unauthorized persons to recover ePHI from the media.

2. Physical Destruction. An alternative to data sanitization of electronic media is physical destruction. The physical destruction of electronic media may be feasible where the media is inexpensive and the destruction methods are easy and safe. The Security Officer or designee must approve the physical destruction of electronic media if such physical destruction is a variation from the Destruction/Disposal of PHI Policy and Procedure.

C. Questions. Questions concerning the destruction/disposal of ePHI should be directed to the Security Officer.

D. Documentation. The City of Sheboygan shall maintain a log of all destruction/sanitization actions as set forth in the Destruction/Disposal of PHI Policy and Procedure and Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(d)(2)(i) – Device and Media Controls; Disposal NIST Special Publication 800-88 – Guidelines for Media Sanitization Destruction/Disposal of PHI Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXIV. DEVICE AND MEDIA CONTROLS: MEDIA RE-USE

1. PURPOSE

To establish procedures for removal of ePHI from electronic media before the media are made available for re-use.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to erase all ePHI from electronic media associated with The City of Sheboygan's information systems before they are made available for re-use. All ePHI on The City of Sheboygan's information systems and associated electronic media will be removed before the systems and media can be re-used.

B. Applicability. Information systems and electronic media to which this Policy applies include, but are not limited to, desktops, laptops, PDAs, tablets, The City of Sheboygan-issued cell phones, hard disks, SAN disks, SD and similar cards, floppy disks, backup tapes, CD\DVD-ROMs, zip drives, portable hard drives, and flash memory devices (thumb drives).

3. PROCEDURE

A. Required Sanitization. Prior to re-use of any electronic media that contained ePHI, the media must be sanitized as set forth in the Device and Media Controls: Disposal Policy and Procedure.

B. Documentation. The City of Sheboygan shall maintain a log of all destruction/sanitization actions as set forth in the Destruction/Disposal of PHI Policy and Procedure and Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(d)(2)(ii) – Device and Media Controls; Media Re-Use Device and Media Controls: Disposal Policy and Procedure Destruction/Disposal of PHI Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXV. DEVICE AND MEDIA CONTROLS: ACCOUNTABILITY

1. PURPOSE

To establish procedures for appropriately tracking and logging the movement of ePHI on information systems and associated electronic media into, out of, and within The City of Sheboygan's facilities.

2. POLICY

The City of Sheboygan commits to maintaining a record of the movements of hardware and electronic media and any person responsible, when appropriate.

3. PROCEDURE

A. Inventory. The City of Sheboygan will maintain an inventory of all information systems and associated devices that store ePHI. Such inventory will include a record of location and assigned User, when appropriate. The City of Sheboygan will maintain a record of the movement of information systems and associated media containing ePHI as they move into and out of The City of Sheboygan's facilities.

B. Movement of Information Systems/Electronic Media. Before information systems and associated media containing ePHI are moved to a location outside of The City of Sheboygan's premises, the move will be approved by The City of Sheboygan, and the movement will be tracked and documented by the Security Officer.

C. Workforce Responsibility.

1. Workforce members who will move the information systems or associated electronic media containing ePHI will be responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized Access.

2. Workforce members are prohibited from removing equipment from The City of Sheboygan unless explicitly approved by the Security Officer. The data and equipment are The City of Sheboygan's property and no Workforce member is entitled to it for personal use.

D. Documentation. The City of Sheboygan shall maintain the inventory of information systems in compliance with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.310(d)(2)(iii) – Accountability Retention of HIPAA Documentation Policy and Procedure; Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator

Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be revised whenever reviewed, even if no changes were made.

XXVI. DEVICE AND MEDIA CONTROLS: DATA BACKUP AND STORAGE

1. PURPOSE

To establish procedures to regularly back up and securely store information available in computing systems and associated electronic media and to regularly test backup and restoration procedures.

2. POLICY

The City of Sheboygan will create a retrievable, exact copy of ePHI, when needed, before movement of equipment to ensure continued operations in the event of a natural disaster, equipment failure, and/or accidental removal of files and will support the need to retrieve archived information.

3. PROCEDURE

A. Backup copies of all ePHI on information systems and associated electronic media will be done regularly and will be stored in a secure location as outlined in the Contingency Plan: Data Backup Plan Policy and Procedure.

B. Backup and restoration procedures for information systems and associated electronic media will be regularly tested to ensure that they are effective and can be completed within a reasonable amount of time consistent with the Contingency Plan: Data Backup Plan Policy and Procedure.

C. Backup media containing ePHI at a remote backup storage site will be given an appropriate level of physical and environmental protection consistent with the standards applied to the protection of ePHI at The City of Sheboygan.

D. The retention period for backup of ePHI on information systems is set forth in the Contingency Plan: Data Backup Plan Policy and Procedure.

References	45 C.F.R. § 164.310(d)(2)(iv) – Data Backup and Storage Contingency Plan: Data Backup Plan Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXVII. UNIQUE USER IDENTIFICATION

1. PURPOSE

To establish procedures for The City of Sheboygan's information systems that require unique names or identifiers for tracking the identity of Users who Access information systems containing ePHI.

2. POLICY

The City of Sheboygan commits to ensure that only authorized persons are granted Access to and can Access its information systems containing ePHI.

3. PROCEDURE

A. **User Authentication.** The City of Sheboygan will utilize User authentication mechanisms for Access to information systems.

B. **Unique User ID.** The City of Sheboygan will assign each Workforce member a unique name and/or number for identifying and tracking User identity. By the assignment of a unique name and/or number, it is the intent of The City of Sheboygan to be able to uniquely identify, monitor, and track a User or Workforce member's Access to networks, systems, and applications and report discrepancies. (See Confidentiality and Information Access Agreement.)

C. **Privilege Level.** Unique identifiers do not give any indication of the User's privilege level.

D. **Sharing of User ID.** Workforce members shall not share assigned unique system identifiers or log-in credentials with any other person unless for authorized support purposes.

E. **Anonymous Access Prohibited.** Anonymous Access, including the use of guest and public accounts, to any The City of Sheboygan-owned information system is prohibited.

F. **User Name and Password.** Passwords shall correspond to each unique User name and should not be shared.

G. **Compensating Controls.** When The City of Sheboygan is not able to implement User IDs for specific applications, The City of Sheboygan will implement appropriate compensating controls, such as maintaining a list of personnel with Access to and knowledge of the credentials used to Access the application and changing the "generic" credentials used to Access the specific application whenever a person with knowledge of the credentials transfers to or is no longer employed by The City of Sheboygan.

H. Log-in Management. The City of Sheboygan's log management tool monitors log-in attempts and discrepancies and the Director of Information Technology timely (daily) monitors the log management tool.

References	45 C.F.R. § 164.312(a)(2)(i) – Unique User Identification Sanction and Discipline Policy and Procedure
Attachments	Confidentiality and Information Access Agreement
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXVIII. EMERGENCY ACCESS PROCEDURE

1. PURPOSE

To establish procedures for an emergency Access procedure enabling authorized Workforce members to obtain ePHI during an emergency.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to having an emergency Access procedure enabling authorized Workforce members to obtain required ePHI during an emergency.

B. Minimum Elements. At a minimum, the procedure will include procedures to:

1. Identify and define manual and automated methods to be used by authorized Workforce members to Access ePHI during an emergency;

2. Identify and define appropriate logging and auditing that must occur when authorized Workforce members Access ePHI during an emergency; and

3. Identify the necessary ePHI that would need to be obtained during an emergency. Such information will be consistent with that identified under The City of Sheboygan's Facility Access Controls: Contingency Operations Policy and Procedure.

3. PROCEDURE

A. Emergency Access Procedure. See Contingency Plan: Disaster Recovery Plan Policy and Procedure and Contingency Plan: Emergency Mode Operations Plan Policy and Procedure for more information regarding The City of Sheboygan's emergency Access procedure.

B. Testing. The City of Sheboygan will test the emergency Access controls to ensure availability and appropriate restrictions. See Contingency Plan: Testing and Revision Procedures Policy and Procedure for The City of Sheboygan's testing process.

C. Records. In the event of emergency, a record will be maintained of systems Accessed.

D. Documentation. The City of Sheboygan shall maintain documentation of its emergency Access procedure consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 312(a)(2)(ii) – Emergency Access Procedure Facility Access Controls: Contingency Operations Policy and Procedure Contingency Plan: Disaster Recovery Plan Policy and Procedure Contingency Plan: Emergency Mode Operations Plan Policy and Procedure Contingency Plan: Testing and Revision Procedures Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXIX. AUTOMATIC LOGOFF

1. PURPOSE

To establish procedures to lock inactive electronic sessions for information systems which contain or Access ePHI.

2. POLICY

The City of Sheboygan commits to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity on information systems that contain ePHI.

3. PROCEDURE

A. User Initiated Logoff. All Workforce members will be required to log off or lock their Workstations prior to leaving the Workstation unattended.

B. Access Termination Period. Workstations, servers, and other computer systems located in open, common, or otherwise insecure areas that Access, transmit, receive, or store sensitive or restricted information, including ePHI, must employ inactivity timers or automatic logoff mechanisms that terminate a User session after a period of inactivity. The inactivity timer or automatic logoff mechanism should terminate the session after no longer than 15 minutes but shall be set for periods of 30 minutes or less in areas of high traffic or that are easily accessible to the public.

C. Systems without Automatic Logoff Capacity. If a system that requires the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:

1. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism;

2. The system must be moved into a secure environment; or

3. All sensitive or restricted information must be removed and relocated to a system that supports an inactivity timer or automatic logoff mechanism.

References	45 C.F.R. § 164.312(a)(2)(iii) – Automatic Logoff Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXX. ENCRYPTION AND DECRYPTION

1. PURPOSE

To establish procedures to implement mechanisms to encrypt and decrypt ePHI to protect the Confidentiality, Integrity, and Availability of ePHI.

2. POLICY

The City of Sheboygan commits to encrypt ePHI as determined to be necessary through a risk analysis process.

3. PROCEDURE

A. Encryption Based on Risk Analysis.

1. Encryption and decryption may be utilized in combination with other Access controls where indicated by risk analysis.

2. The following factors will be considered in determining the encryption requirement for specific ePHI:

    a. The sensitivity of the ePHI;

    b. The risks to the ePHI;

    c. The expected impact to functionality and work flow if the ePHI is encrypted; and

    d. Alternative methods available to protect the Confidentiality, Integrity, and Availability of the EPHI.

3. The Security Officer will review the risk analysis report to identify systems that require ePHI to be encrypted.

B. Media Encryption. Media which cannot be protected by other methods of Access control (e.g., passwords) shall utilize encryption and decryption to protect ePHI from unauthorized Disclosure.

C. Encryption Standards. Proven, standard algorithms will be used for encryption technologies. The City of Sheboygan's encryption standards, e.g., encryption mechanisms should support a minimum of 128-bit AES encryption. See Transmission Security Policy and Procedure for The City of Sheboygan's transmission encryption standards.

D. Encryption Testing. The Security Officer will test encryption and decryption capabilities of products and systems to ensure proper functionality. Such testing will be documented in the auditing and monitoring records.

E. Documentation. The City of Sheboygan shall maintain documentation of its encryption standards consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.312(a)(2)(iv) – Encryption and Decryption Transmission Security Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXI. AUDIT CONTROLS

1. PURPOSE

To establish procedures to implement appropriate hardware, software, or procedural mechanisms which record and examine significant activity on information systems that contain or use ePHI and to ensure activities within The City of Sheboygan's information systems that contain or use ePHI are recorded and monitored for signs of tampering/misuse.

2. POLICY

A. **The City of Sheboygan's Commitment.** The City of Sheboygan commits to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

B. **Significant Activity.** The City of Sheboygan will record and examine significant activity on its information systems that contain or use ePHI. The City of Sheboygan will identify, define, and document what constitutes "significant activity" on a specific information system. Such activity will include:

1. User Access to ePHI and User account activity;
2. Use of certain software programs or utilities;
3. Use of a privileged account;
4. Computing system anomalies, such as unplanned system shutdown or application errors; or
5. Failed and successful authentication attempts.

C. **Audit Mechanisms.** Appropriate hardware, software, or procedural auditing mechanisms will be implemented on all systems that contain or use ePHI. At a minimum, such mechanisms have to provide the following information:

1. Date and time of activity;
2. Origin of activity;
3. Identification of User performing activity; and
4. Description of attempted or completed activity.

D. **Audit Review Process.** The City of Sheboygan will develop and implement a formal process for audit log review. At a minimum, the process will include:

1. Definition of which Workforce members will review records of activity;
2. Definition of what activity is significant;

3. Procedures defining how significant activity will be identified and reported; and

4. Procedures for preserving records of significant activity.

3. PROCEDURE

A. Review of Records of System Activity.

1. The Security Officer and IT Department are responsible for reviewing the records of system activities. Systems that contain ePHI may include Workstations, laptops, servers, personal data assistants, other computing systems and electronic media.

2. When possible, Workforce members will not review audit logs that pertain to their own system activity.

3. Workforce members will not have the ability to alter or delete log entries that pertain to their own system activity. If it is not possible to limit this access, management will ensure that appropriate compensating controls are documented and implemented.

4. The Security Officer or designee will notify Workforce members that their activities are monitored by an audit trail.

B. SIEM Product. The City of Sheboygan has adopted a Security Information and Event Management ("SIEM") product to assist in the auditing and collection of various security logs. Those systems containing ePHI that are not included in the SIEM product are audited manually. The audit logs provide the Security Officer with a chronological trail of computer events that gives information about an operating system, an application, or User Access. The audit trail will be used to monitor computer activity to assist in determining:

1. Whether a Security Incident has occurred;

2. Whether there is an indication of unauthorized Access;

3. Whether there is unusual Workforce member Access; and

4. Whether there is unusual activity that requires further investigation.

C. Activities Identified with Audit Log Review. The following activities may be identified through review of audit logs:

1. Users Accessing more information than they are authorized to Access;

2. Prolonged log-in;

3. Prolonged logoff;

4. Sharing of passwords by identifying the same password on more than one Workstation;

5. A User ID logging into the system at an unusual Workstation site (see Unique User Identification Policy and Procedure);

6. Access that is inappropriate for the User assigned to the User ID (see Unique User Identification Policy and Procedure);

7. Downloading of files or Accessing information that is inappropriate for The City of Sheboygan business environment or assigned job functions; and

8. Running programs that interfere with the efficiency of the system.

D. Logged Activity. The following are examples of logged activity in information systems:

1. User access log;

2. User activity log;

3. Administrator access log;

4. Administration activity log;

5. Facility access log; and

6. Data backup log.

E. Documentation.

1. When possible, audit trails will be stored on a separate service to maintain the Confidentiality of the audit trail.

2. The audit trails will be accessible only to the Security Officer. The City of Sheboygan has the ability to document tracking at the application level, computer level, computer network level, or server-based activity (User and file folder).

References	45 C.F.R. § 164.312(b) – Audit Controls Unique User Identification Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXII. MECHANISM TO AUTHENTICATE ePHI

1. PURPOSE

To establish procedures to implement appropriate electronic mechanisms to confirm that ePHI contained on The City of Sheboygan's computing systems has not been altered or destroyed in an unauthorized manner.

2. POLICY

The City of Sheboygan commits to implement appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

3. PROCEDURE

A. Mechanism to Authenticate ePHI. Electronic mechanisms used to protect the Integrity of ePHI contained on The City of Sheboygan's computing systems are implemented to ensure the value and state of the ePHI are maintained, and data is protected from unauthorized modification and destruction. Such mechanisms will also be capable of detecting unauthorized alteration or destruction of ePHI. Such mechanisms will include, but are not limited to:

1. System memory, hard drives, and other data storage devices with error-detection capabilities;

2. File and data checksums;

3. Encryption.

References	45 C.F.R. § 164.312(c)(2) – Mechanism to Authenticate ePHI Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXIII. PERSON OR ENTITY AUTHENTICATION

1. PURPOSE

To establish procedures for authenticating all persons or entities seeking Access to The City of Sheboygan's ePHI before Access is granted. Authentication is done through an appropriate and reasonable system(s) so that only properly authorized persons or entities can Access ePHI.

2. POLICY

The City of Sheboygan will make a reasonable effort to verify that a person or entity seeking Access to ePHI is who they claim to be and is appropriately authenticated before Access is granted.

3. PROCEDURE

A. Internal Person or Entity Authentication. The City of Sheboygan will ensure Workforce member authentication via the assignment of User ID and password requirements. (See Unique User Identification Policy and Procedure and Password Management Policy and Procedure.)

B. External Person or Entity Authentication. The following procedures are to be utilized for authenticating all Users (persons or entities, as appropriate) requesting Access to PHI:

1. Physical Access. The City of Sheboygan will utilize a sign-in sheet for verification of identification at the front door for visitors/vendors that may need Access to the network or any applications that may contain ePHI.

2. Information System Access.

   a. All persons or entities that need to Access PHI will be first authorized to Access that data before having an account established on any information system.

   b. Whenever a person or entity is authorized to Access such information, only the Minimum Necessary information required to perform their designated function is to be authorized for Access. (See Minimum Necessary Requirements Policy and Procedure.)

C. Authentication Mechanisms. Authentication mechanisms may include, as appropriate, but are not limited to, the following:

1. User name and password;

2. Biometrics;

3. Challenge and response mechanisms;

4. Secure identification cards;

5. Sample text.

References	45 C.F.R. § 164.312(d) – Person or Entity Authentication Unique User Identification Policy and Procedure Password Management Policy and Procedure Minimum Necessary Requirements Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXXIV. INTEGRITY CONTROLS

1. PURPOSE

To establish procedures for implementing appropriate Integrity controls to protect the Confidentiality, Integrity, and Availability of The City of Sheboygan's ePHI transmitted over electronic communications networks to ensure the value and state of all transmitted ePHI are maintained and data is protected from unauthorized modifications.

2. POLICY

A. The City of Sheboygan's Commitment. The City of Sheboygan commits to using appropriate Integrity controls to protect the Confidentiality, Integrity, and Availability of The City of Sheboygan's ePHI transmitted over electronic communications networks. The City of Sheboygan also utilizes various methods to protect ePHI from improper and/or unauthorized alteration or destruction and validates that this has not happened until properly disposed of according to the Device and Media Controls: Disposal Policy and Procedure.

B. Integrity Controls. Integrity controls may include, but are not limited to:

1. Encryption;

2. Checksums;

3. Point-to-point communications, such as Virtual Private Networks (VPN); and

4. Switched networks.

3. PROCEDURE

A. Determination of Integrity Controls. The City of Sheboygan uses Integrity controls that are reasonable and appropriate to protect the Confidentiality, Integrity, and Availability of The City of Sheboygan's ePHI transmitted over electronic communications networks. The appropriateness of controls is based upon the sensitivity of and risks to ePHI.

B. Integrity Controls. The City of Sheboygan will utilize the following reasonable methods to ensure data Integrity:

1. Users, during the regular course of their job responsibilities, are required to check for and report any errors or potential errors of ePHI identified in information systems to the Security Officer.

2. Physical Safeguards and Technical Safeguards are in place to prevent unauthorized Access to Workstations and information systems as described in this HIPAA Policies and Procedures Manual. (See, e.g., Information

Access Management Policy and Procedure; Access Establishment, Modification, and Review Policy and Procedure; Log-In Monitoring Policy and Procedure; Facility Access Controls: Contingency Operations Policy and Procedure; Facility Access Controls: Security Plan Policy and Procedure; Facility Access Controls: Access Control and Validation Policy and Procedure; Unique User Identification Policy and Procedure; Password Management Policy and Procedure; Computer Terminals/Workstations Policy and Procedure; Workstation Use Policy and Procedure; Workstation Security Policy and Procedure; Automatic Logoff Policy and Procedure; Encryption and Decryption Policy and Procedure; Person or Entity Authentication Policy and Procedure.)

3. Audit trails on information systems and Workstations are in place to identify all changes made to ePHI as described in the Audit Controls Policy and Procedure.

4. Backup external hard drives are used to restore any possible data loss. (See Contingency Plan: Data Backup Plan Policy and Procedure.)

5. The Security Officer ensures that information systems are tested for accuracy and functionality before using them in the live environment. In addition, before integrating ePHI from one information system to another, the data is validated. (See System Build/Change Control Policy and Procedure.)

6. While completing a risk analysis, The City of Sheboygan considers various risks to the Integrity of ePHI and identifies security measures to reduce risks. (See Risk Analysis and Risk Management Policy and Procedure.)

7. Encryption and other mechanisms to secure information are utilized to prevent transmission errors and unauthorized Access to PHI. (See Transmission Security Policy and Procedure.)

8. The City of Sheboygan uses software products that indicate corrected or improved versions.

    a. All systems have currently been programmed to receive automatic Windows updates.

    b. Where appropriate, a system update server/patch management server has been implemented to automatically update systems to the most recent version.

9. Antivirus software, or other programs designed to identify malicious software, are installed and updated. (See Protection from Malicious Software Policy and Procedure.)

References	45 C.F.R. § 164.312(c)(1) – Integrity Device and Media Controls: Disposal Policy and Procedure Information Access Management Policy and Procedure Access Establishment, Modification, and Review Policy and Procedure Log-In Monitoring Policy and Procedure Facility Access Controls: Contingency Operations Policy and Procedure Facility Access Controls: Security Plan Policy and Procedure Facility Access Controls: Access Control and Validation Policy and Procedure Unique User Identification Policy and Procedure Password Management Policy and Procedure Computer Terminals/Workstations Policy and Procedure Workstation Use Policy and Procedure Workstation Security Policy and Procedure Automatic Logoff Policy and Procedure Encryption and Decryption Policy and Procedure Person or Entity Authentication Policy and Procedure Contingency Plan: Data Backup Plan Policy and Procedure Audit Controls Policy and Procedure System Build/Change Control Policy and Procedure Risk Analysis and Risk Management Policy and Procedure Transmission Security Policy and Procedure Protection from Malicious Software Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXXV. TRANSMISSION SECURITY

1. PURPOSE

To establish procedures for implementing security measures which will ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of and to establish procedures for appropriate encryption of PHI transmitted through electronic communication networks.

2. POLICY

A. Encryption. The City of Sheboygan will make a reasonable effort to guard against unauthorized Access to ePHI transmitted over an electronic communications network to prevent interception, redirection, and/or modification of information transmitted by/to The City of Sheboygan over an electronic communications network. The following factors will be considered in determining whether encryption must be used when sending specific ePHI over an electronic communications network:

1. The sensitivity of the ePHI;
2. The risks to the ePHI;
3. The expected impact to functionality and workflow if the ePHI is encrypted; and
4. Alternative methods available to protect the Confidentiality, Integrity, and Availability of the ePHI.

(See Encryption and Decryption Policy and Procedure.)

B. Transmission. The City of Sheboygan commits to ensure that only authorized persons are granted Access and can Access ePHI transmitted over an electronic communications network.

3. PROCEDURE

A. Encryption. Any ePHI transmitted inbound/outbound from The City of Sheboygan is appropriately encrypted.

1. Secure tunnel – password protected.
2. Traffic between sites is not permitted.
3. All information with ePHI is encrypted.

B. Internal ePHI Transmission. Workforce members e-mailing ePHI, including any link to ePHI, within The City of Sheboygan shall:

1. Ensure the e-mail is correctly addressed;

2. Ensure any attachments are appropriate for the addressee;

3. Add the encryption trigger "Confidential: Contains PHI" to the e-mail subject line; and

4. Click "Encrypt and Send" from the Outlook e-mail window.

C. External ePHI Transmission. To appropriately guard against unauthorized Access to or modification of ePHI that is being transmitted from The City of Sheboygan's network to an outside network, the following procedures are utilized:

1. All transmissions of ePHI from The City of Sheboygan's network to a network outside of the organization will utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing ePHI will be encrypted before transmission;

2. The receiving person or entity will be authenticated prior to transmitting ePHI through electronic transmission networks (see Person or Entity Authentication Policy and Procedure);

3. All transmission of ePHI from The City of Sheboygan's network to a network outside will include only the Minimum Necessary amount of PHI; and

D. ePHI Transmission Using Electronic Removable Media. When transmitting ePHI via removable media, including, but not limited to, floppy disks, CD-ROM, memory cards, magnetic tape, removable hard drives, etc., the sending party must:

1. Use an encryption mechanism to protect against unauthorized Access or modification;

2. Authenticate the person or entity requesting ePHI (see Person or Entity Authentication Policy and Procedure); and

3. Send the Minimum Necessary amount of ePHI required by the receiving person or entity. (See Minimum Necessary Requirements Policy and Procedure.)

E. ePHI Transmissions Using Wireless LANs and Devices. The transmission of ePHI over a wireless network within The City of Sheboygan's networks is permitted if the following conditions are met:

1. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized;

2. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network; and

3. If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.

F. Receipt of ePHI. Workforce members will request that any ePHI being sent to The City of Sheboygan will be sent in a password-protected and/or encrypted file. Workforce members will ask that the password be sent in a separate e-mail. Files that are unable to be decrypted will be handled on a case-by-case basis.

G. Workforce Responsibility. When transmitting ePHI electronically, regardless of the transmission system being used, all Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the ePHI requested.

References	45 C.F.R. § 164.312(e)(1) – Transmission Security 45 C.F.R. § 164.312(e)(2)(i) – Integrity Controls 45 C.F.R. § 164.312(e)(2)(ii) – Encryption Person or Entity Authentication Policy and Procedure Encryption and Decryption Policy and Procedure Minimum Necessary Requirements Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXVI. STORAGE OF DOCUMENTS

1. PURPOSE

To establish procedures to store documents containing PHI from unauthorized Access.

2. POLICY

The City of Sheboygan commits that physical storage of documents containing PHI will be done so that they are protected from unauthorized Access, whether inadvertent or otherwise.

3. PROCEDURE

A. Storage of Documents. Documents containing PHI shall be stored in locked file cabinets separate from other documents (e.g., personnel files) to which authorized individuals may appropriately have Access. The file cabinets shall be located in a secure location.

B. Access Limitation. Authorized Workforce members are granted Access to specific information. Such Access is limited to specific, denied, documented, and approved applications and level of Access rights.

C. File Cabinets. Authorized Workforce members may not leave file cabinets containing PHI documents unlocked or unattended for long periods of time (e.g., breaks, lunch, meetings, etc.). File cabinets must be locked at the end of the work shift. Authorized staff will not:

1. Provide the key of any file cabinet containing PHI documents to other Workforce members or third parties; and

2. Allow other Workforce members or third parties Access to such file cabinets.

References	45 C.F.R. § 164.530 – Administrative Requirements Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XXXVII. DE-IDENTIFICATION OF PHI

1. PURPOSE

To establish the process of de-identifying PHI in accordance with HIPAA and guidance issued by HHS so that the information will no longer be considered PHI.

Also, to establish process for removing certain identifying information from PHI in order to create a Limited Data Set that may be Disclosed for Research, public health, or Health Care Operations purposes with the recipient of the Limited Data Set entering into a Data Use Agreement with the Covered Entity that restricts the way in which the Limited Data Set can be Used and Disclosed.

2. POLICY

Whenever possible, The City of Sheboygan shall Use and Disclose De-identified Health Information rather than PHI. The City of Sheboygan commits to de-identification of PHI, when appropriate, in accordance with HIPAA and guidance issued by HHS.

3. PROCEDURE

A. Creation of De-identified Data. The City of Sheboygan may Use PHI to create De-identified Data, in compliance with this Policy and the HIPAA Rules regarding creation of De-identified Data.

B. De-Identification Methods. The City of Sheboygan will use one of two methods for de-identification of PHI:

1. Statistician Determination. A biostatistician with appropriate knowledge and experience in applying generally accepted statistical and scientific principles and methods for making information not individually identifiable determines that the risk is very small that the information could be Used (either by itself, or in combination with other available information) by anticipated recipients to identify an Individual.

    a. If this method of de-identification is used, the analytical methods used and results of the analysis must be documented and documentation must be retained.

2. Removing Identifiers. All of the following identifiers of the Individual or of the relatives, employers, or household members of the Individual are removed:

    a. Names;

    b. Geographic subdivision, such as street address, city, county, and zip code;

c. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and, if it has fewer than 20,000 people, the zip code is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate);

d. All elements of dates (except year) for dates directly related to the Individual, including birth date, admission date, discharge date, date of death; all ages over 89; and all elements of dates (including year) indicative of such age;

e. Telephone numbers;

f. Fax numbers;

g. E-mail addresses;

h. Social Security Numbers;

i. Medical record numbers;

j. Health Plan beneficiary numbers;

k. Account numbers;

l. Certificate/license numbers;

m. Vehicle identifiers, serial numbers, license plate numbers;

n. Device identifiers and serial numbers;

o. Web Universal Resource Locators (URLs);

p. Internet Protocol (IP) address numbers;

q. Biometric identifiers, including fingerprints and voiceprints;

r. Full face photographic images and other comparable images; and

s. All other unique identifying numbers, characteristics, or codes.

Once all elements are removed, The City of Sheboygan must confirm that it has no actual knowledge that the residual information can be used to identify the Individual.

It is the responsibility of The City of Sheboygan to ensure that all identifiers are removed in accordance with these requirements.

C. Re-Identification. The City of Sheboygan may assign a code that would allow the De-identified Data to be re-identified as long as the code is not derived from or related to information about the Individual and is not otherwise capable of being translated so as to identify the Individual.

1. The City of Sheboygan will not Use or Disclose the code or any other means of record identification for any other purpose and must not Disclose the mechanism for re-identification.

2. Whenever possible, the code will be encrypted and maintained securely. Under no circumstances will The City of Sheboygan maintain the code on the same server as the De-Identified Health Information.

3. If De-identified Data is re-identified, such re-identified information is PHI and may be Used and Disclosed only as permitted or required by HIPAA and The City of Sheboygan's HIPAA Policies and Procedures Manual.

References	45 C.F.R. § 164.502(d) – Uses and Disclosures of De-Identified Protected Health Information 45 C.F.R. §§ 164.514(a)-(b) – De-Identification of PHI 45 C.F.R. § 164.530 – Administrative Requirements Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXVIII. MAIL: INTERNAL AND EXTERNAL

1. PURPOSE

To establish procedure guidelines for safeguarding PHI from inappropriate Use or Disclosure of PHI when mailing such information.

2. POLICY

The City of Sheboygan utilizes both internal and external mail (i.e., postal service and delivery services) to deliver data on a routine basis. The City of Sheboygan will provide physical and procedural Safeguards to minimize the possibility of unauthorized observation or Access to PHI during the mailing of data.

3. PROCEDURE

A. **Addresses.** The person sending mail containing PHI will double-check the accuracy of the mail address of the addressee before sending the mail.

B. **Envelopes.** When PHI is mailed (internal or external), no PHI shall be included on the envelope, nor shall it be visible through the envelope, including any window in the envelope. With respect to internal mail, only the recipient's name shall be indicated on the envelope.

C. **Secure Envelopes.** When PHI is mailed (internal or external), it should be mailed in a sealed envelope or an envelope that may be securely closed, and it should not be provided to unauthorized staff or third parties (e.g., mail room staff) until properly sealed or closed. To the extent it is impractical to place it in a secure envelope, interoffice mail may be transmitted without an envelope, provided that the first page of the mail does not contain PHI (i.e., a cover page is used or the first page is turned over) and PHI is not otherwise visible.

D. **Mail Recipient.** Only authorized Workforce members shall open mail that is received (internal or external mail source) when it is likely the mail contains PHI. To the extent mail is received in an envelope that is not addressed to a specific person, when it is unclear that it is from the subject of PHI, or when it is unclear whether it may contain PHI, the mail may be opened by unauthorized staff, provided that person opening the envelope reviews the least amount of contents needed to determine to whom the mail is addressed and/or that it contains PHI, at which time the mail should be delivered to the appropriate person.

References	45 C.F.R. § 164.530 – Administrative Requirements Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XXXIX. COPY MACHINES

1. PURPOSE

To establish and implement Physical Safeguards and Administrative Safeguards to minimize the possibility of unauthorized Access to PHI during copying of data.

2. POLICY

A. The City of Sheboygan utilizes copy machines to copy data on a routine basis. The City of Sheboygan also occasionally utilizes third-party copy services to copy data. The City of Sheboygan will use Physical Safeguards and Administrative Safeguards to minimize the possibility of unauthorized observation or Access to PHI during the copying of data.

B. This Policy outlines the required elements for a secure location of a copy machine and establishes guidelines for how The City of Sheboygan will reasonably safeguard PHI during copying to limit incidental or accidental Use or Disclosure of PHI.

3. PROCEDURE

A. **Location.** Copy machines used to copy PHI shall be placed in a secure location. If possible, copy machines used to copy PHI will not be used regularly for other purposes.

B. **Removal of Original Documents.** After copying any document containing PHI, the person making the copies will double-check to confirm that no original documents containing PHI are left on or at the copy machine.

C. **Removal of PHI Document Copies.** After copying any document containing PHI, the person making the copies will double-check to confirm that none of the copies containing PHI are left on or at the copy machine.

D. **Erase Memory.**

1. If the copy machine is equipped with storage memory that allows the re-printing of a document previously copied, the person making the copies of documents containing PHI will delete the memory and double-check that the memory has been deleted prior to leaving the copy machine.

2. The Security Officer or his/her designee will delete the memory of all copy machines used to copy PHI when decommissioned.

E. **Destruction of Copies.** In the event a copy containing PHI is unusable, it is to be destroyed consistent with The City of Sheboygan's Destruction/Disposal of PHI Policy and Procedure. The person making the copy will destroy the copy, regardless of whether it is legible.

F. **Unattended Copying.** In no instance shall the person making copies of documents containing PHI leave the copier unattended while copies are being made.

G. **Outsourcing.** Prior to providing documents/data containing PHI to any such copy service for copying, the copy service must sign a business associate agreement with The City of Sheboygan consistent with The City of Sheboygan's Business Associate Agreements Policy and Procedure. Additionally, the mail policy shall be followed with respect to delivering the original documents/data to the copy service.

References	45 C.F.R. § 164.530 – Administrative Requirements Destruction/Disposal of PHI Policy and Procedure Business Associates and Business Associate Agreements Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

XL. E-MAIL

1. PURPOSE

To establish procedures for sending e-mails containing PHI in a secured manner as per HIPAA.

2. POLICY

The City of Sheboygan utilizes electronic mail (e-mail) in transmitting PHI electronically. Established security measures must be followed by all Workforce members who have the authority to transmit PHI electronically.

3. PROCEDURE

A. Authorized User. Authorized User is defined as a person who has:

1. Been assigned a User ID (see Unique User Identification Policy and Procedure); and

2. The authority to read, enter, or update information created or transmitted by The City of Sheboygan.

B. Personal Use.

C. Improper Use. Improper use of e-mail and internet services is strictly prohibited. Examples of such improper use include, but are not limited to:

1. Sending/forwarding harassing, insulting, defamatory, obscene, offending or threatening messages;

2. Gambling, surfing, or downloading pornography;

3. Downloading or sending PHI without proper authorization;

4. Copying or transmission of any document software or other information protected by copyright and/or patent law, without proper authorization;

5. Transmission of highly sensitive or confidential information (e.g., HIV status, mental illness, chemical dependency, workers' compensation claims, etc.);

6. Obtaining access to files or communication of others without proper authorization;

7. Attempting unauthorized Access to Individual or The City of Sheboygan data;

8. Attempting to breach any security measure on any The City of Sheboygan electronic communication system(s);

9. Attempting to intercept any electronic communication transmission without proper authorization;

10. Misrepresenting, obscuring, suppressing, or replacing an authorized User's identity;

11. Using e-mail addresses for Marketing purposes without permission from Security Officer and the Privacy Officer;

12. Using e-mail system for solicitation of funds, political messages, or any other illegal activities; and

13. Releasing of passwords and User IDs.

D. **E-mails are Property of The City of Sheboygan.** E-mails originated or received into The City of Sheboygan e-mail system are considered to be the property of The City of Sheboygan and, therefore, are subject to the review and monitoring of the Privacy Officer and/or Security Officer or designee. The City of Sheboygan reserves the right to access employee e-mail (whether present or not) for the purposes of ensuring the protection or Confidentiality of Individual or The City of Sheboygan information.

E. **Inadvertent Access.** During routine maintenance, upgrades, problem resolution, etc., information systems technician(s) may inadvertently Access User e-mail communications. Such staff, when carrying out their assignments, will not intentionally read or disclose content of e-mail unless such data is found to be in violation of The City of Sheboygan's HIPAA Policies and Procedures Manual.

F. **Protection of Information.** Users of the e-mail system must ensure that all information forwarded, distributed, or printed is protected according to The City of Sheboygan's HIPAA Policies and Procedures Manual.

G. **E-mail Response.** When an e-mail message containing PHI is received, any reply or response to that message (i.e., an acknowledgement of receipt of the message) should not include the PHI received whenever possible. E-mail systems often automatically include the sender's e-mail message when a reply is made. When the original message includes PHI, the original message should be manually removed from the reply prior to sending any reply whenever possible.

H. **E-mail Forward.** When an e-mail message containing PHI is received, any forward of that message (whether internal or external) should not include the PHI received whenever possible. E-mail systems automatically include the sender's e-mail message when a forward is made. When the original message includes PHI, the PHI in the original message should be manually removed from the forward prior to sending any forward whenever possible.

I. Individual's Request for Plain E-Mail. An Individual or his/her representative has the right to request that such Individual or his/her representative communicate with The City of Sheboygan using unencrypted, unsecured e-mail or other technology that may be in use at The City of Sheboygan. If an e-mail with unencrypted PHI is received from an Individual or his/her representative, or if such Individual or his/her representative requests to use plain e-mail, The City of Sheboygan must explain that plain e-mail is not secure and obtain consent to use insecure technology at the request of the Individual. Any consents should be documented, and any PHI in unencrypted e-mail should be minimized to reduce any impacts of possible exposure.

J. Archiving E-mails. E-mail messages may not be maintained or archived for more than 30 days, unless otherwise approved by the Privacy Officer. Information that should be retained longer than 30 days for purposes of medical records or compliance must be archived with the approval of the Privacy Officer.

References	45 C.F.R. § 164.530 – Administrative Requirements Unique User Identification Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

XLII. MOBILE DEVICES: OWNED BY THE CITY OF SHEBOYGAN

1. PURPOSE

To provide guidance for the security of Mobile Devices owned by The City of Sheboygan.

2. DEFINITIONS

For the purpose of this Policy, "Mobile Device(s)" include all electronic computing and communications devices that may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information – whether directly through download or upload, text entry, photograph, or video – from any data source – whether through wireless, network, or direct connection to a computer, other portable device, or any equipment capable of recording, storing, or transmitting digital information (e.g., smartphones, digital music players, hand-held computers, tablet computers, laptop computers, and personal digital assistants).

3. POLICY

The City of Sheboygan commits to using reasonable methods to protect the security of The City of Sheboygan-owned Mobile Devices.

4. PROCEDURE

A. Authorization to Use Mobile Devices.

1. No Mobile Device may be used for any purpose or activity involving PHI without prior registration of the Mobile Device and written authorization by the Security Officer. Authorization will be given only for use of Mobile Devices that the IT Department has confirmed have been configured so that the Mobile Devices comply with this Policy.

2. Authorization to use a Mobile Device may be suspended or terminated at any time:

    a. If the User fails or refuses to comply with this Policy;

    b. In order to avoid, prevent or mitigate the consequences of a violation of this Policy;

    c. In connection with the investigation of a suspected or actual Breach, Security Incident, or violation of The City of Sheboygan's HIPAA Policies and Procedures Manual or other applicable policies and procedures;

    d. In order to protect Individual life, health, privacy, reputational or financial interests;

e. In order to protect any assets, information, reputational or financial interests of The City of Sheboygan;

f. Upon request of the supervisor or head of the department in which the User works; or

g. Upon the direction of the Security Officer.

3. Authorization to use a Mobile Device terminates:

a. Automatically upon the termination of a User's status as a member of The City of Sheboygan's Workforce;

b. Upon a change in the User's role as a member of The City of Sheboygan's Workforce, unless continued authorization is requested by the supervisor or head of the department in which the User works; and

c. If it is determined that the User violated this Policy or any other The City of Sheboygan policy or procedure, in accordance with The City of Sheboygan's Sanction and Discipline Policy and Procedure.

4. The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.

B. Security Guidelines. In order to protect The City of Sheboygan Mobile Devices from unintended or intended exposure of PHI, The City of Sheboygan and Workforce members will adhere to the following Mobile Device security guidelines:

1. The City of Sheboygan's Workforce members using Mobile Devices shall consider the sensitivity of the information, including PHI that may be Accessed and minimize the possibility of unauthorized Access;

2. Only authorized personnel will have physical access to The City of Sheboygan Mobile Devices;

3. Mobile device management software ("MDM") will be installed on all The City of Sheboygan Mobile Devices. MDM software must be capable of, at a minimum, encryption tracking, remote wiping, and enforcing device-level password security;

4. Device encryption will be required on all The City of Sheboygan Mobile Devices;

5. Device passwords will be required on all The City of Sheboygan Mobile Devices;

6. Device passwords will be changed on a regular basis;

7. Automatic remote wiping after 10 failed log-ins will be enforced on the Mobile Device for those Mobile Devices that support it;

8. The City of Sheboygan Mobile Device users will comply with all applicable password policies and procedures (see Password Management Policy and Procedure);

9. All The City of Sheboygan Mobile Devices are to be used for authorized business purposes only;

10. Software installations must be approved by the IT Department and performed by IT Department. File sharing applications will not be installed on Mobile Devices;

11. Under no circumstances will The City of Sheboygan confidential information be stored on a The City of Sheboygan Mobile Device;

12. Mobile Devices should not be used to Access or transmit PHI on a public wireless network unless the User uses secure, encrypted connections;

13. To avoid physical damage to a Mobile Device due to accidental spills, all food and drink should be kept at a safe distance;

14. The City of Sheboygan Mobile Devices that are to be removed from production permanently to be sold or recycled will be reset to factory settings and removable media destroyed (see Device and Media Controls: Disposal Policy and Procedure and Device and Media Controls: Media Re-Use Policy and Procedure); and

15. The loss or theft of any The City of Sheboygan Mobile Device must be reported to IT Department immediately.

C. Personal Use of Mobile Devices. All information on a Mobile Device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by The City of Sheboygan to the extent it deems reasonably necessary:

1. In order to avoid, prevent or mitigate the consequences of a violation of this Policy;

2. In connection with the investigation of a potential or actual Breach, Security Incident, or violation of The City of Sheboygan policies and procedures;

3. In order to protect the life, health, privacy, reputational or financial interests of any Individual;

4. To protect any assets, information, reputational or financial interests of The City of Sheboygan;

5. For purposes of determining sanctions against the User or any other member of The City of Sheboygan's Workforce pursuant to the Sanction and Discipline Policy and Procedure;

6. For purposes of litigation involving the User or The City of Sheboygan; and

7. If Required by Law.

D. Audit of Mobile Devices. Upon request by the IT Department or the Security Officer, at his/her/its sole discretion at any time, any Mobile Device may be subject to audit to ensure compliance with this and other The City of Sheboygan policies. Any User receiving such a request shall transfer possession of the Mobile Device to the IT Department at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.

References	45 C.F.R. § 164.530 – Administrative Requirements NIST Special Publication 1800 – Mobile Device Security HHS Guidance on Mobile Device and Health Information Privacy and Security, available at: https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security Password Management Policy and Procedure Device and Media Controls: Disposal Policy and Procedure Device and Media Controls: Media Re-Use Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	to be revised whenever reviewed, even if no changes were made.
Revisions	to be updated whenever revisions are made, keeping record of *all* revision dates.

XLIII. MOBILE DEVICES: WORKFORCE-OWNED (BYOD)

1. PURPOSE

To provide guidance for the security of Workforce-owned Mobile Devices when the Mobile Device is used to Access e-mail or any PHI supplied by The City of Sheboygan.

2. DEFINITIONS

For the purpose of this Policy, "Mobile Device(s)" include all electronic computing and communications devices that: (1) are owned by Workforce member(s); (2) may be used to Access e-mail or any PHI supplied by The City of Sheboygan; and (3) may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information – whether directly through download or upload, text entry, photograph, or video – from any data source – whether through wireless, network, or direct connection to a computer, other portable device, or any equipment capable of recording, storing, or transmitting digital information (e.g., smartphones, digital music players, hand-held computers, tablet computers, laptop computers, and personal digital assistants).

3. POLICY

The City of Sheboygan commits to using reasonable methods to protect the security of Workforce-owned Mobile Devices used to Access e-mail or any PHI supplied by The City of Sheboygan.

4. PROCEDURE

A. Authorization to Use Mobile Devices to Access E-mail or Any PHI Supplied by The City of Sheboygan.

1. No Workforce member may use a Mobile Device to Access e-mail or any PHI supplied by The City of Sheboygan without written authorization by the IT Department, Security Officer or his/her designee. Authorization will be given only for use of Mobile Devices that the IT Department has confirmed have been configured so that the Mobile Devices comply with this Policy.

2. Authorization must be requested for each Mobile Device the Workforce member may use to Access e-mail or PHI supplied by The City of Sheboygan.

3. Authorization to use a Mobile Device to Access e-mail or any PHI supplied by The City of Sheboygan may be suspended or terminated at any time:

    a. If the User fails or refuses to comply with this Policy;

    b. In order to avoid, prevent or mitigate the consequences of a violation of this Policy;

c. In connection with the investigation of a suspected or actual Breach, Security Incident, or violation of The City of Sheboygan's HIPAA Policies and Procedures Manual or other applicable policies and procedures;

d. In order to protect Individual life, health, privacy, reputational or financial interests;

e. In order to protect any assets, information, reputational or financial interests of The City of Sheboygan;

f. Upon request of the supervisor or head of the department in which the User works; or

g. Upon the direction of the Security Officer.

4. Authorization to use a Mobile Device to Access e-mail or any PHI supplied by The City of Sheboygan terminates:

a. Automatically upon the termination of a User's status as a member of The City of Sheboygan's Workforce;

b. Upon a change in the User's role as a member of The City of Sheboygan's Workforce, unless continued authorization is requested by the supervisor or head of the department in which the User works; and

c. If it is determined that the User violated this Policy or any other The City of Sheboygan policy or procedure, in accordance with The City of Sheboygan's Sanction and Discipline Policy and Procedure.

5. The use of a Mobile Device to Access e-mail or any PHI supplied by The City of Sheboygan without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.

B. Security Guidelines. In order to protect Mobile Devices from unintended or intended exposure of PHI, The City of Sheboygan and Workforce members will adhere to the following Mobile Device security guidelines:

1. The City of Sheboygan's Workforce members using Mobile Devices shall consider the sensitivity of the information, including PHI that may be Accessed and minimize the possibility of unauthorized Access.

2. Mobile device management software ("MDM") will be installed on all Mobile Devices if the User intends to Access e-mail or any PHI supplied by The City of Sheboygan. MDM software must be capable of, at a minimum, encryption tracking, remote wiping, and enforcing device-level password security.

3. Device encryption will be required on all Workforce-owned Mobile Devices that are used to Access e-mail or any PHI supplied by The City of Sheboygan.

4. Device passwords will be required on all Workforce-owned Mobile Devices that are used to Access e-mail or any PHI supplied by The City of Sheboygan.

5. Device passwords will be changed on a regular basis.

6. Automatic remote wiping after 10 failed log-ins will be enforced on the Mobile Device for those Mobile Devices that support it.

7. The City of Sheboygan Mobile Device users will comply with all applicable password policies and procedures. (*See* Password Management Policy and Procedure.)

8. Installation of software that can be used to Access e-mail or any PHI supplied by The City of Sheboygan must be approved by the Security Officer.

9. Users may not transmit PHI with any file sharing applications.

10. Under no circumstances will The City of Sheboygan confidential information be stored on a Mobile Device.

11. Mobile Devices should not be used to Access or transmit PHI on a public wireless network unless the User uses secure, encrypted connections.

12. When a User plans a Mobile Device upgrade or plans, for any reason, to sell, transfer, or stop using a Mobile Device, the User will provide Mobile Devices to Security Officer to confirm that The City of Sheboygan confidential information and PHI is not accessible via any software on the Mobile Device. (See Device and Media Controls: Disposal Policy and Procedure and Device and Media Controls: Media Re-Use Policy and Procedure.)

13. The loss or theft of any Mobile Device must be reported to the IT Department immediately. In the event that a Mobile Device is confirmed lost or stolen, the Mobile Device will be remotely wiped.

References	45 C.F.R. § 164.530 – Administrative Requirements NIST Special Publication 1800 – Mobile Device Security HHS Guidance on Mobile Device and Health Information Privacy and Security, available at: https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security Password Management Policy and Procedure Device and Media Controls: Disposal Policy and Procedure Device and Media Controls: Media Re-Use Policy and Procedure

	Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

41457605_2.DOCX

CITY OF SHEBOYGAN
HIPAA POLICIES AND PROCEDURES MANUAL

VOLUME 4:
INCIDENT AND BREACH INVESTIGATION AND NOTIFICATION

ADOPTED: _____

TABLE OF CONTENTS[1]

[1] *Exhibits are provided in a separate document.*

I. PRIVACY AND SECURITY INCIDENT RESPONSE AND REPORTING

1. PURPOSE

To establish consistent guidelines for the City of Sheboygan to handle privacy and security incidents.

2. POLICY

The City of Sheboygan is dedicated to preventing, detecting, containing, and correcting privacy and security incidents. The City of Sheboygan has implemented an incident response process to consistently detect, report, respond to, and investigate incidents, minimize loss and destruction, mitigate any weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

3. PROCEDURE

A. Preparation.

1. The City of Sheboygan Security Incident response team is composed of Privacy Officer.

2. The City of Sheboygan conducts regular training and awareness of Security Incident responses, including but not limited to periodic testing of the City of Sheboygan's Security Incident response procedures.

3. All actions to respond to and recover from Security Incidents are carefully and formally controlled. At a minimum, the City of Sheboygan's Security Officer will ensure that:

    a. All actions taken are intended to minimize the damage of a Security Incident and prevent further damage; and

    b. Only authorized and appropriately trained Workforce members or the City of Sheboygan Business Associates are allowed to access affected information systems in order to respond to or recover from a Security Incident.

B. Identification Phase.

1. <u>Reporting</u>.

    a. All Workforce members are expected to report any of the following as soon as possible and in no case later than 24 hours from complaint, known incident, or suspected incident:

        i. Known or suspected Security Incidents, Breaches, inappropriate Uses or Disclosures of PHI;

ii. Known or suspected violations of the City of Sheboygan's HIPAA Policies and Procedures Manual;

iii. Complaints from an Individual or another entity/individual regarding the City of Sheboygan's handling of PHI or the City of Sheboygan's Workforce member's compliance with the City of Sheboygan's HIPAA Policies and Procedures Manual; or

iv. Any other concerns regarding the privacy or security of PHI.

b. Reporting any known or suspected privacy or security issues is considered a contribution toward quality improvement. There will be no retaliation for reporting privacy or security issues consistent with the City of Sheboygan's Refraining From Intimidating or Retaliatory Acts Policy and Procedure.

c. Reporting should be directed to the HIPAA Privacy Officer and Security Officer. In the absence of the HIPAA Privacy Officer and Security Officer, or in the event of the HIPAA Privacy Officer and Security Officer's potential involvement, reporting should be directed to the City Administrator.

d. Reporting may be done by email, voicemail, in writing, phone, in person verbally, or any other appropriate method.

2. Investigation. Confidentiality of PHI will be maintained while investigating, reporting, and responding to privacy and security issues. Documentation of any privacy and/or security issue is to be kept secure to prevent additional exposure.

a. Upon receipt of a report, the Privacy Officer and/or Security Officer, as appropriate, shall:

i. Determine if the report relates to a potential or suspected inappropriate Use or Disclosure of PHI.

ii. For reports that are both privacy- and security-related, the Privacy Officer and Security Officer shall work together to complete required investigation obligations.

iii. If the event is identified as a privacy incident that resulted in a reportable Breach of Unsecured PHI, refer to the City of Sheboygan's Breach Investigation and Notification Policy and Procedure.

b. The City of Sheboygan has not violated the requirements of the Privacy Rule if:

i. A Workforce member that is a victim of a criminal act Discloses relevant PHI to a law enforcement official, provided that the PHI Disclosed is about the suspected perpetrator of the criminal act and the minimum necessary PHI Disclosed is limited to: Name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and/or description of distinguishing physical characteristics.

ii. A Workforce member or a Business Associate believes in good faith that the City of Sheboygan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the City of Sheboygan potentially endanger one or more Individuals, workers, or the public and the Disclosure is made to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the City of Sheboygan or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the City of Sheboygan.

C. Privacy Incident Complaint Procedure.

1. The HIPAA Privacy Officer is designated as the individual responsible for receiving, processing, and investigating all privacy related complaints/incidents. The HIPAA Privacy Officer may in turn designate Workforce members in particular areas to assist.

2. Any Individual, Personal Representative, family member, Workforce member, Business Associate, visitor, or the general public may file a grievance or complaint regarding the City of Sheboygan's policies and/or practices without fear of reprisal or retaliation in any form. (See Refraining From Intimidating or Retaliatory Acts Policy and Procedure.)

3. Written complaints should be submitted to the HIPAA Privacy Officer. The HIPAA Privacy Officer or his/her designee will timely begin an investigation into allegations after receipt of the complaint.

4. Move to Completion of Privacy Incident Report and Security Incident Report Forms Phase and Follow-Up Phase.

D. Security Incident Containment Phase. The City of Sheboygan's Security Officer and applicable Workforce members shall quickly and efficiently contain the Security Incident.

1. The Security Officer or designee, in collaboration with appropriate Workforce members, facilitates the following, as applicable:

    a. Verifies that a qualified technical security resource is available to assist with efforts;

    b. Evaluates the need to use forensic analysis;

    c. Secures the physical and network perimeter:

        i. If a decision is made to remove the system from the network for eradication, containment, and/or investigative purposes, consults with the City of Sheboygan's Information Technology Director.

        ii. Before the decision to freeze the system is made, volatile data must be taken from the system while it is still in its compromised state whenever possible. The physical area where the Security Incident occurred must be physically secured. Care should be taken not to alert any intruder to the actions.

        iii. Removes the network cable from the affected system. Do not reboot or make any changes to the system itself.

    d. Retrieves any volatile data from the affected system;

    e. Secures attached User accounts to prevent further unauthorized Access;

    f. Determines the relative Integrity and the appropriateness of backing up the system:

        i. If appropriate, backs up the system.

        ii. Protects backups and logs them (refer to the City of Sheboygan's Contingency Plan: Data Backup Plan Policy and Procedure).

    g. Changes the password(s) to the affected system(s);

    h. Determines whether it is safe to continue operations with the affected system(s):

        i. If it is safe, allows the system to continue to function. Complete documentation as described below and move to the Follow-Up Phase.

ii. If it is not safe to allow the system to continue operations, discontinue system(s) operation and move to Eradication Phase.

i. Analyzes the data and determines whether or not to initiate an alert to the City of Sheboygan's Users.

j. Issues alerts as deemed necessary.

2. The Security Officer keeps the Privacy Officer apprised of progress and documents all measures taken and communications made, including the start and end times of all efforts, on the Security Incident Report Form in a clear and easy to understand way.

E. Security Incident Eradication Phase. The City of Sheboygan shall remove the causes, and the resulting security exposures, that are now on the affected system(s).

1. The Security Officer or designee, in collaboration with appropriate members of the Workforce, facilitates the following, as applicable:

a. Determines symptoms and causes related to the affected system(s);

b. Strengthens the defense surrounding the affected system(s), where possible (a risk assessment may be needed). This may include the following:

i. An increase in network perimeter defenses;

ii. An increase in system monitoring defenses;

iii. Remediation ("fixing") of any security issues within the affected system, such as removing unused services/general host hardening techniques, firewall/router changes, vulnerability patches applied, physical access control changes, etc.

c. Conducts a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed. (See Risk Analysis and Risk Management Policy and Procedure.) If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.

2. The Security Officer keeps the City of Sheboygan's Privacy Officer apprised of progress and documents all measures taken and communications made, including the start and end times of all efforts, on the Security Incident Report Form in a clear and easy to understand way.

3. Refer to the City of Sheboygan's Breach Investigation and Notification Policy and Procedure to determine whether the City of Sheboygan must provide notification of incident.

4. Continue to Follow-up Phase.

F. Security Incident Recovery Phase. The City of Sheboygan shall restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The Security Officer or designee, in collaboration with appropriate Workforce members, determines if the affected system(s) has been changed in any way and, as applicable:

   a. Restores the system(s) to proper, intended functioning (last known good).

      i. Once restored, validates that the system functions in a way that it was intended/had functioned in the past. This may require involvement of the business unit that owns the affected system(s).

      ii. If operation to the system(s) has been interrupted (i.e., the system(s) was taken offline or dropped from the network while triaged), restarts the restored and validated system(s) and monitors for proper behavior.

   b. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restarts the system and monitors for proper behavior.

   c. Ensures the system is using latest configuration standards.

   d. Performs a vulnerability assessment and penetration using the City of Sheboygan-approved software and method as described in the Risk Analysis and Risk Management Policy and Procedure.

   e. Update system monitoring if necessary to alert to the specific vulnerability or attack in the future.

2. The HIPAA Security Officer keeps the Privacy Officer apprised of progress and documents all measures taken and communications made, including the start and end times of all efforts in a clear and easy to understand way.

3. Continue to Completion of Privacy Incident Report and Security Incident Report Forms Phase and Follow-Up Phase.

G. Completion of Privacy Incident Report and Security Incident Report Forms. For privacy-related reports, a Privacy Incident Report Form must be completed in a clear and easy to understand way. For security-related reports, a Security Incident Report Form must be completed in a clear and easy to understand way.

1. If, after an analysis as set forth in the Breach Investigation and Notification Policy and Procedure, the issue was a privacy incident, the City of Sheboygan will report the findings of the investigation to the individual filing the complaint within thirty (30) days of receiving such complaint unless an extension is necessary to complete the investigation. Such report will include the result of the investigation, the recommended resolution, and contact information for the Secretary. If the individual is not satisfied with the result of the investigation or the recommended resolution, he/she may file a complaint with the Secretary.

2. If the issue was or is potentially a Security Incident, proceed as follows:

    a. For Cyber-Related Security Incidents (as defined in the Addressing Cyber-Related Security Incidents Policy and Procedure), proceed to the Addressing Cyber-Related Security Incidents Policy and Procedure and then complete the Follow-Up Phase below.

    b. For other Security Incidents, move to the Follow-Up Phase below.

3. If the incident was the result of the City of Sheboygan's Workforce member's action/inaction, refer to the City of Sheboygan's Sanction and Discipline Policy and Procedure.

H. Follow-Up Phase. Review the Privacy Incident Report Form or Security Incident Report Form to look for "lessons learned" and determine whether the incident handling procedures could have been done in a better way.

1. It is recommended that all incidents be reviewed shortly after resolution to determine where response could be improved for future issues.

2. The Privacy Officer, Security Officer or designee(s), in collaboration with appropriate members of the City of Sheboygan's Workforce, shall review the incident documentation and complete the following (as applicable and appropriate):

    a. Evaluate the cost and impact of the incident to the City of Sheboygan;

    b. Determine what could be improved to prevent a similar incident from occurring in the future;

    c. Create a "lessons learned" summary and attach it to the completed Privacy Incident Report and/or Security Incident Report Forms;

d. Communicate findings to the City of Sheboygan's City Administrator for approval and for implementation of any recommendations;

e. Carry out recommendations approved by the City of Sheboygan's City Administrator.

3. Close the incident.

I. Documentation. the City of Sheboygan shall maintain any documentation related to privacy incident and/or Security Incident reporting and response consistent with the Retention of HIPAA Documentation Policy and Procedure. Documentation shall include, at a minimum:

1. Name of person reporting incident;

2. Name of person(s) conducting the incident response investigation;

3. Description of the data and the information system(s) affected by the incident;

4. Date and time of incident;

5. Damage to data and the information system(s);

6. Suspected cause of the incident;

7. Identified risk;

8. Actions taken to mitigate the damage and restore the data and/or information system(s); and

9. Recommendations for further actions to enhance the security of ePHI.

References	45 C.F.R. § 164.308(a)(1) – Security Management Process 45 C.F.R. § 164.308(a)(6)(i) – Security Incident Procedures 45 C.F.R. § 164.308(a)(6)(ii) – Security Incident Response and Reporting 45 C.F.R. § 164.512(f)(2) – Disclosures for Law Enforcement Purposes 45 C.F.R. § 164.530(d)(1-2) – Complaints to Covered Entity Refraining From Intimidating or Retaliatory Acts Policy and Procedure Breach Investigation and Notification Policy and Procedure Risk Analysis and Risk Management Policy and Procedure Addressing Cyber-Related Security Incidents Policy and Procedure Contingency Plan: Data Backup Plan Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	Privacy Incident Report Form Security Incident Report Form
Responsible Senior Leaders	Privacy Officer, Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	to be revised whenever reviewed, even if no changes were made.
Revisions	to be updated whenever revisions are made, keeping record of ***all*** revision dates.

II. ADDRESSING CYBER-RELATED SECURITY INCIDENTS

1. PURPOSE

To establish the City of Sheboygan's procedures for quickly and effectively detecting and responding to a Cyber-Related Security Incident.

2. DEFINITIONS

"Cyber-Related Security Incident" means a Security Incident that was an attempt to compromise the electronic security perimeter or physical security perimeter of a critical cyber asset. A Cyber-Related Security Incident also includes a Security Incident that disrupted or attempted to disrupt the operation of those programmable electronic devices and communications networks, including hardware, software and data that are essential to the operation of an information system.

3. POLICY

The City of Sheboygan is committed to implementing policies and procedures to quickly and effectively address Cyber-Related Security Incidents that may affect the Confidentiality, Integrity, or Availability of PHI.

4. PROCEDURE

A. **Security Incident Response.** The City of Sheboygan maintains a documented process for quickly and effectively detecting and responding to Security Incidents that may impact the Confidentiality, Integrity, or Availability of PHI (see Privacy and Security Incident Response and Reporting Policy and Procedure).

B. **Reporting Cyber-Related Security Incidents.** After the City of Sheboygan executes a response, mitigation, and contingency plan consistent with the City of Sheboygan's Privacy and Security Incident Response and Reporting Policy and Procedure and Contingency Plan: Data Backup Plan Policy and Procedure, the Security Officer shall report the following, as applicable:

1. Crimes.

   a. The City of Sheboygan shall report crimes to law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation, and/or the Secret Service, as appropriate. Any such reports should not include PHI, unless otherwise permitted by the Privacy Rule.

   b. If a law enforcement official tells the City of Sheboygan that any potential Breach report would impede a criminal investigation or harm national security, the City of Sheboygan will delay reporting a Breach for the time the law enforcement requests in writing, or for 30 days if the request is made orally. See also the City of

Sheboygan's Breach Investigation and Notification Policy and Procedure.

2. Cyber Threat Indicators. The City of Sheboygan shall assess whether it needs to report cyber threat indicators to federal and information-sharing and analysis organizations ("ISAOs") (e.g., the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private sector cyber-threat ISAOs). Any such reports should not include PHI.

3. Breach. Refer to the City of Sheboygan's Breach Investigation and Notification Policy and Procedure to determine whether the City of Sheboygan must provide notification of an incident as a Breach of Unsecured PHI.

C. Documentation. The City of Sheboygan shall maintain any documentation related to the responding, controlling, reporting, monitoring, investigating, and sanctioning of Cyber-Related Security Incidents consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.308(a)(6)(i) – Security Incident Procedures OCR Cyber Attack Checklist, *available* https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf (Last accessed 12/05/2017) Privacy and Security Incident Response and Reporting Policy and Procedure Contingency Plan: Data Backup Plan Policy and Procedure Breach Investigation and Notification Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Privacy Officer, Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

III. BREACH INVESTIGATION AND NOTIFICATION

1. PURPOSE

To establish the City of Sheboygan's procedures for identification of a Breach of Unsecured PHI by the City of Sheboygan and its Business Associate(s) and provide required notifications to Individuals, prominent media, and HHS, as appropriate, within the timeframe Required by Law.

2. DEFINITIONS

Capitalized terms used but not defined in this Policy shall have the meaning set forth in the City of Sheboygan's HIPAA Policies and Procedures Manual Glossary.

3. POLICY

A. Breach Assessment. The City of Sheboygan is dedicated to safeguarding the Confidentiality, Integrity, and Availability of PHI through an established incident response process. The City of Sheboygan will evaluate each reported potential Breach of Unsecured PHI by following the City of Sheboygan's Privacy and Security Incident Response and Reporting Policy and Procedure. If a privacy issue and/or a Security Incident is identified, the City of Sheboygan will determine the probability that PHI has been compromised and what additional action is required.

B. Breach Notification. The City of Sheboygan timely addresses Breaches of Unsecured PHI in compliance with the HIPAA Breach Notification Rule.

4. PROCEDURE

A. Breach Risk Assessment. The Privacy Officer will determine whether there has been a Breach of Unsecured PHI by completing the following:

1. Notify the City of Sheboygan's City Administrator of a privacy issue and/or a Security Incident, containing the Breach to prevent further unauthorized Disclosure if possible.

2. Complete a Breach risk assessment using the Breach Risk Assessment Tool to determine whether one of the following has occurred:

    a. The privacy/Security Incident is not a Breach and, therefore, no notification is required.

    b. A reportable Breach of Unsecured PHI has occurred. Notification to the Individual who is the subject of the Unsecured PHI and HHS is required under the Breach Notification Rule. Notification to the media may also be required. See below: Notification to Individuals, Notification to HHS, and Notification to the Media.

c. A state-defined violation that is not a HIPAA Breach of Unsecured PHI has occurred, i.e., a violation that does not meet the HIPAA Breach notification requirements but does meet a state-specific Breach notification requirement has occurred. Notification is required under state law. Consult with legal counsel regarding state notification requirements (e.g., Wis. Stat. § 134.98 et seq.).

d. A state-defined violation and HIPAA Breach of Unsecured PHI has occurred, i.e., a violation that potentially requires notification under HIPAA and state Breach notification requirements has occurred. Consult with legal counsel regarding appropriate compliance response. See below: Notification to Individuals, Notification to HHS, and Notification to the Media.

e. No state-defined violation or HIPAA Breach of Unsecured PHI has occurred, but a possible the City of Sheboygan HIPAA policy and procedure violation has occurred. No notification is required. Determine whether disciplinary action, HIPAA policy and procedure revisions, and/or the City of Sheboygan Workforce retraining is needed.

3. Exceptions to Breach Notification. Breach notification is necessary in all Breaches of Unsecured PHI except where the City of Sheboygan or the City of Sheboygan's Business Associate demonstrates that there is a low probability that the PHI has been compromised or when one of the following exceptions applies:

a. The unintentional acquisition, access, or Use of PHI by a Workforce member or person acting under the authority of the City of Sheboygan or the City of Sheboygan's Business Associate, if such acquisition, access, or Use was made in good faith and within the scope of authority.

b. An inadvertent Disclosure of PHI by a person authorized to access PHI at the City of Sheboygan or the City of Sheboygan's Business Associate to another person authorized to access PHI at the City of Sheboygan or the City of Sheboygan's Business Associate or OHCA in which the City of Sheboygan participates. In both cases, the information cannot be further Used or Disclosed in a manner not permitted by the Privacy Rule.

c. The City of Sheboygan or the City of Sheboygan's Business Associate has a good faith belief that the unauthorized person to whom the impermissible Disclosure was made would not have been able to retain the information.

4. Business Associate and Subcontractor Responsibilities. The City of Sheboygan's Business Associates that create, receive, maintain, transmit, access, retain, modify, record, store, destroy or otherwise hold, Use or Disclose PHI are required, upon discovery of any Breach of PHI, to notify the City of Sheboygan without unreasonable delay, in no case later than 10 days after discovery of a Breach.

   a. The notification must include the identification of each Individual whose PHI has been, or is reasonably believed to have been, Breached and, at the time of notification, or as soon as the information becomes available, information as outlined below in Content of Notification.

   b. The City of Sheboygan's Privacy Officer will coordinate the investigation, Breach assessment and notification process for any Breach that is identified by the City of Sheboygan's Business Associate or Business Associate's Subcontractor. Unless set forth otherwise in a BAA, the City of Sheboygan will determine who is in the best position to provide Breach notification to HHS, the media as necessary, and the Individual, and will work with Business Associate to ensure the Individual receives just one notice (vs. notice from the City of Sheboygan and Business Associate).

   c. The City of Sheboygan will attempt to use the City of Sheboygan's template BAA with Business Associates such that Business Associates are required to report all Uses and Disclosures of PHI not specifically authorized by the BAA rather than just Breaches of Unsecured PHI. (See Business Associates and Business Associate Agreements Policy and Procedure and Template Business Associate Agreement (For Use When the City of Sheboygan is the Covered Entity).)

5. Burden of Proof. In the event the City of Sheboygan determines a privacy issue and/or Security Incident did not result in a Breach of Unsecured PHI, the City of Sheboygan shall have the burden of demonstrating that the Use or Disclosure did not constitute a Breach. The Breach Risk Assessment Worksheet must be entirely completed and the conclusion that Breach notification is not required must be well supported.

B. Notification by a Business Associate.

1. If a Breach of Unsecured PHI occurs at or by a Business Associate, the Business Associate must notify the Privacy Officer following the discovery of the Breach. A Business Associate must provide notice to the City of Sheboygan as set forth in the BAA.

2. If a Business Associate suffers a Breach, the Privacy Officer may consider the Breach discovered when the Business Associate notifies the City of Sheboygan.

3. If the City of Sheboygan receives notification from a Business Associate regarding the occurrence of a Breach of Unsecured PHI, the City of Sheboygan shall conduct a Breach risk assessment as set forth in this Policy and proceed to the notification phase if the City of Sheboygan determines the incident is a reportable Breach of Unsecured PHI.

4. Upon completion of all required notifications, the City of Sheboygan will assess what, if any, additional mitigation, legal action, or compliance assessments are required in order to continue a relationship with the Business Associate or Subcontractor that caused the Breach.

C. Date of Discovery. A Breach shall be treated as discovered by the City of Sheboygan as of the first day on which such Breach is known to the City of Sheboygan or, by exercising reasonable diligence, would have been known to the City of Sheboygan. The City of Sheboygan shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the City of Sheboygan (determined in accordance with the federal common law of agency).

D. Breach Notification. If the City of Sheboygan determines, via a Breach risk assessment, that a Breach of Unsecured PHI has occurred, the City of Sheboygan will proceed to Breach notification.

Notification to Affected Individuals, the Secretary and the Media. If the Breach occurred while the City of Sheboygan was acting in the capacity of a Covered Entity, the City of Sheboygan will provide notice to the affected Individual(s), HHS, and the media (as necessary) as set forth below.

1. Notification to Individuals. the City of Sheboygan shall use the Template Breach Notification Letter Form and proceed as follows:

   a. *Written Notice* – without unreasonable delay, and in no case later than 60 days from the date discovered, the City of Sheboygan shall mail a Breach Notification Letter, via first class mail, to all affected Individuals (or the Individual's Personal Representative, as applicable).

      i. If the Individual indicated agreement to the City of Sheboygan for electronic notice and such agreement has not been withdrawn, the written notice may be sent via electronic mail.

ii. In situations where notification is required by both HIPAA and state law, the City of Sheboygan shall submit one notification letter satisfying the earliest of the applicable due dates and all required elements of both regulating entities.

iii. In any case deemed to require urgency because of possible imminent misuse of PHI, the City of Sheboygan will provide information to Individuals by phone call or other means, as appropriate, in addition to the written notice described above.

b. *Substitute Notice* – If there is insufficient or out-of-date contact information that prevents written notification to:

i. *Fewer than 10 Individuals* – a substitute form of notice (e.g., telephone call) will be utilized.

ii. *10 or more Individuals* – a substitute notice, in the form of a conspicuous posting for a period of 90 days on the City of Sheboygan's website home page or conspicuous notice in a major print or broadcast media where the affected Individuals are likely to reside. The conspicuous notice to 10 or more Individuals will include a toll-free number that remains active for at least 90 days where an Individual can learn whether his/her Unsecured PHI may be included in the Breach.

2. Notification to the Media. If the Breach affects more than five hundred (500) residents of a state or jurisdiction, in addition to notifying the affected Individuals, the City of Sheboygan is required to provide notice to prominent media outlets serving the state or jurisdiction. the City of Sheboygan will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. This media notification must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a Breach of Unsecured PHI and must include the same information required for the Individual notice.

a. The City of Sheboygan shall use the Template Media Breach Notification Release Form and proceed as follows for those single Breaches of Unsecured PHI involving 500 or more Individuals:

i. Notify prominent media outlets serving the area in question.

ii. This notice shall be done without unreasonable delay, and in no case later than 60 calendar days after discovery, and will include information available as outlined in Content of Notification section of this Policy and Procedure.

3. Notification to the Secretary. The City of Sheboygan shall provide notification to HHS using the HHS Breach Notification Template Form, proceeding as follows:

   a. *500 or More Individuals* – For Breaches of Unsecured PHI involving 500 or more Individuals, the City of Sheboygan will provide notice to the Secretary without unreasonable delay, and in no case later than 60 calendar days after discovery. HHS only accepts notification of Breaches under HIPAA via the online HHS reporting process.

   b. *Fewer than 500 Individuals* – For Breaches of Unsecured PHI involving fewer than 500 Individuals, the City of Sheboygan will maintain a log of Breaches of Unsecured PHI and, not later than 60 calendar days after the end of each calendar year, provide HHS a notification for Breaches discovered during the preceding calendar year in a manner specified on the HHS web site.

4. Law Enforcement Delay. In the event a law enforcement official states that a notification, notice or posting of a Breach, as required by HIPAA, would impede a criminal investigation or cause damage to national security, the City of Sheboygan shall do the following if:

   a. The statement was made orally, the City of Sheboygan shall document the statement, identity of the official making the statement, and delay the action no longer than 30 days from the date of the oral statement, unless a written statement, as described below, is submitted.

   b. The statement was in writing and specifies the time for which a delay is required – delay action for the time period specified.

5. Content of Notification. The notification should be in plain language and must include all of the following:

   a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

   b. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

   c. Any steps which Individuals should take to protect themselves from potential harm resulting from the Breach (i.e., place a fraud alert on credit report);

d. A brief description of what the City of Sheboygan is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches;

e. Contact procedures for Individuals to ask questions or learn additional information, via a toll-free number, an email address, website, or portal address.

E. Documentation. In order to demonstrate all notifications are made as required by HIPAA, the City of Sheboygan will maintain a generic copy of any notification (paper or electronic; to the Individual, media, Secretary) and an Excel listing of the affected Individuals and how each was notified, or how notification was attempted (i.e., media). The City of Sheboygan shall maintain all documentation related to Breach notification consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.414 – Burden of Proof 45 C.F.R. § 164.410(b) – Notification by a BA - Timeliness of Notification 45 C.F.R. § 164.412 – Law Enforcement Delay 45 C.F.R. § 164.404(a) – Notification to Individuals 45 C.F.R. § 164.404(c) – Content of Notification 45 C.F.R. § 164.406(a) – Notification to the Media 45 C.F.R. § 164.408(a) – Notification to the Secretary 45 C.F.R. § 164.410(a) – Notification by a Business Associate 45 C.F.R. § 164.414(b) – Burden of Proof Business Associates and Business Associate Agreements Policy and Procedure Template Business Associate Agreement (For Use When the City of Sheboygan is the Covered Entity)
Attachments	HIPAA Breach Risk Assessment Tool Template Breach Notification Letter Template Media Breach Notification Release HHS Breach Notification Template Breach Log
Responsible Senior Leaders	Privacy Officer, Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of ***all*** revision dates.

IV. DUTY TO MITIGATE

1. PURPOSE

To establish the City of Sheboygan's procedures to mitigate any harmful effect of a Use or Disclosure of PHI in violation of the City of Sheboygan's HIPAA Policies and Procedures Manuals or the HIPAA Rules.

2. POLICY

The City of Sheboygan will mitigate, to the extent practicable, any harmful effect that is known to the City of Sheboygan of a Use or Disclosure of PHI in violation of the City of Sheboygan's HIPAA Policies and Procedures Manuals or the HIPAA Rules. The City of Sheboygan expects its Business Associates to mitigate any Use or Disclosure of PHI in violation of the BAA between the City of Sheboygan and each such Business Associate.

3. PROCEDURE

A. When the City of Sheboygan is made aware of a violation of the City of Sheboygan's HIPAA Policies and Procedures Manuals or the HIPAA Rules, the City of Sheboygan will take the following actions:

1. The HIPAA Privacy Officer/HIPAA Security Officer will be notified and will start an immediate investigation. (See Breach Investigation and Notification Policy and Procedure.)

2. The City of Sheboygan will determine if the violation constitutes a Breach of Unsecured PHI. (See Breach Investigation and Notification Policy and Procedure.)

3. The City of Sheboygan will identify the extent of any violations or Breaches and will take reasonable steps to correct the violation or halt the Breach, if possible, and mitigate any impact of the violation or Breach.

4. The City of Sheboygan will consider training and Workforce education opportunities from the violation or Breach.

5. The City of Sheboygan follow through on any required Breach Notification. (See Breach Investigation and Notification Policy and Procedure.)

B. **Documentation.** The City of Sheboygan shall maintain any documentation consistent with the Retention of HIPAA Documentation Policy and Procedure.

References	45 C.F.R. § 164.530(f) – Mitigation Contingency Plan: Data Backup Plan Policy and Procedure Breach Investigation and Notification Policy and Procedure Retention of HIPAA Documentation Policy and Procedure Sanction and Discipline Policy and Procedure
Attachments	N/A
Responsible Senior Leaders	Privacy Officer, Security Officer, City Administrator
Effective Date	November 4, 2024
Review Dates	N/A, to be revised whenever reviewed, even if no changes were made.
Revisions	N/A, to be updated whenever revisions are made, keeping record of *all* revision dates.

40979237_4.DOCX