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.