City of
Sheboygan
spirit on the lake

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.*

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 <u>contact list</u> 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. <u>Data Sanitization</u>. 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.