CITY OF GREEN BAY PERSONNEL POLICY

Policy Title	Policy Reference
HIPAA Privacy Policy	Chapter 28
Policy Source	**Legal Review Date**
Human Resources Department	April 19, 2018
Personnel Committee Approval	**City Council Approval**
April 24, 2018	May 1, 2018

Policy Reference

All City of Green Bay Departments, Divisions, Operational Areas, Functions, Employees, Officials and other Representatives using or having access to the Protected Health Information (PHI) of any person. This policy includes by specific reference the Human Resources Department; the Parks, Recreation and Forestry Department; the Transit Department; the Wellness Nurse and the City of Green Bay active employee self-insured group health and dental plans. This policy excludes the City of Green Bay Fire Department.

Scope

The City of Green Bay (City) is committed to compliance with the HIPAA Privacy and Security Regulations (Rules) set forth by the U.S. Department of Health and Human Services (HHS). These Rules provide that all protected health information that is received by or generated through a covered entity must be afforded certain protections. Covered entities include health plans, health care providers and health care clearinghouses. The City maintains several health plans that are covered entities. The City also performs certain functions that qualify certain City Departments or staff as health care providers. Accordingly, as an entity that has some covered functions and some non-covered functions, the City will consider itself a hybrid entity, for purposes of and as allowed by the Rules.

This Policy covers the responsibilities and obligations of City of Green Bay Departments, Divisions, Operational Areas, Functions, Employees, Officials and other Representatives, other than the Fire Department, regarding their role in the documentation, designations, policies and procedures and other actions required for compliance with the HIPAA Privacy and Security

Regulations. To the extent any City of Green Bay Department, Division, health plan or other entity could be considered a separate covered entity under the Rules, this Policy designates all such entities as under the common control of the City of Green Bay.

Due to its specific HIPAA compliance obligations, the City of Green Bay Fire Department operates under the City of Green Bay's Fire Department HIPAA Use and Disclosure of Protected Health Information policy. The City's Fire Department HIPAA Policy oversight is provided by the Fire Department's HIPAA Privacy and Security Officer.

Accordingly, all references to the City as a covered entity in this Policy relate to City functions other than the Fire Department. All references to the City's HIPAA Privacy and Security Officer in this Policy relate to the Privacy and Security Officer for City functions other than the Fire Department.

Purpose

To provide a summary of the City's policies and standards with respect to documentation required for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Regulations as amended.

The HIPAA Privacy and Security Regulations require that covered entities maintain documentation of certain decisions, designations, policies and procedures, and other actions taken for purposes of compliance with the regulations. These documentation requirements provide a basis for workforce training, facilitate the creation of the required notice of privacy practices, and enhance accountability for compliance with the Rules.

Policy

It is the City's policy to fully comply with all documentation requirements imposed by the HIPAA Privacy and Security Regulations and under state law. Each City Department or function that operates as a health plan, health care provider or health care clearinghouse shall:

- Develop, maintain and retain the documentation described below in accordance with this policy.
- Develop, document and implement procedures as necessary to ensure compliance with this policy.
- Provide training to appropriate personnel as necessary to ensure satisfaction of these documentation requirements.

Definitions

Protected health information (PHI) means, generally, health information that is individually identifiable (i.e., patient-specific) and that is created, maintained, used or disclosed by or for a City employee, official or representative.

More specifically, the term refers to information that:

(i) identifies or could reasonably be used to identify the individual and
(ii) relates to:
  (a) the individual's physical or mental health or condition,
  (b) the provision of health care to the individual, or
  (c) payment for health care provided to the individual.

For example, protected health information includes information that identifies an individual as a City group health plan participant or that associates a condition, treatment or payment-related information (diagnosis codes, dates of service, charge data, etc.) to information that ***could be*** used to identify the individual (name, description of condition, other demographics, medical record number, insurance claim number, images, etc.).

Electronic protected health information (ePHI) is PHI maintained or transmitted in electronic form. The HIPAA Privacy and Security Regulations do not distinguish between electronic forms of information. Some examples of ePHI are employee health information stored on magnetic tapes or disks, optical disks, hard drives, and servers. Examples of transmission media include Internet and Extranet technology, leased lines, private networks, and removable media such as disks.

The HIPAA Security Rule defines a "security incident" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Procedure

29.1 POLICIES AND PROCEDURES. Policies addressing compliance with privacy and security laws and regulations are developed in accordance with the City's policies on Records and Transaction Management, Electronic Communications and Information Systems Usage and other City and Department-specific data privacy policies. In addition, each City Department will adopt supporting procedures as provided in such policies and otherwise as necessary to enable effective HIPAA compliance policy implementation and workforce training.

PHI and ePHI must be maintained as confidential within City administration and externally to members of the public unless disclosure is allowed by this Policy or required under state or federal law. Daily work activities that require a City employee, official or representative to use or have access to PHI or ePHI of any person must be performed to ensure that access is limited internally and externally to the minimum amount of protected information required to perform an official duty. Use or access that exceeds this limitation may be considered a security incident.

Every instance of a security incident or possible security incident must be reported to and logged by the Privacy and Security Officer, his or her designee or the Department's designated Data Privacy Compliance Officer. Each City employee, official or agent who has or may have access to PHI or ePHI will receive training to ensure understanding of and compliance with the City's data privacy requirements, including HIPAA.

City employees, officials or agents who require access to PHI or ePHI for the purpose of payment for health care, insurance, treatment or health care-related services are allowed to view the information without express authorization from the patient (or the patient's parent if the patient is under 18), unless authorization is required under this Policy, under a City Department Data Privacy policy or by state or federal law.

The Human Resources Director is the City's Privacy and Security Officer under this Policy. The Privacy and Security Officer provides direction and oversight to each City Department and to the Human Resources Department for development of policies specific to the City's employee health benefit plans and provision of health-related services. Such policies may vary from the standards in the City's organization-wide policies as necessary to reflect the differences in regulatory requirements applicable to covered entities that are also self-insured health plans. Similarly, policies and procedures that address compliance for individual City Departments may vary from the organization-wide standards as necessary to reflect the requirements of state and federal law.

Documented policies and procedures related to privacy and security compliance obligations will be modified promptly to comply with changes in relevant laws and regulations, and policy and procedure changes will be implemented within the time required for legal compliance.

The Privacy and Security Officer shall ensure that the City's organization-wide privacy and security compliance policies and procedures are maintained and retained in accordance with this Policy. The Compliance Accountable Manager for each affected

Department, or his or her designee, shall ensure that privacy and security compliance policies and procedures specific to that Department are maintained and retained in accordance with this Policy.

29.2 NOTICE OF PRIVACY PRACTICES. The Privacy and Security Officer will be responsible for developing, with all necessary input from managers within operations and departments and/or vendors, the City's Notice(s) of Privacy Practices. The Human Resources Department will retain copies of the notice(s) issued as documentation of compliance.

The Privacy and Security Officer shall ensure that the City's Notice(s) of Privacy Practices are promptly revised and distributed to City Departments whenever there is a material change to the uses or disclosures, individuals' rights, the City's legal duties or other privacy practices described in the notice(s).

29.3 COMPLAINTS ABOUT PRIVACY AND SECURITY COMPLIANCE PRACTICES. Within each City Department (excluding areas that are not responsible for employee health benefit plans or billing, do not receive or transmit protected health information or do not otherwise receive individuals' complaints in the regular course of business), the designated office or person responsible for receiving complaints relating to privacy and security compliance practices will be responsible for documenting the complaints received and their disposition.

29.4 REPORT OF DISCLOSURES. Each City Department (excluding areas that are not responsible for employee health benefit plans or billing, do not receive or transmit protected health information or do not otherwise receive individuals' complaints in the regular course of business) will document its designation of the persons or offices responsible for receiving and acting on an individual's request for a report (or "accounting") of disclosures of protected health information.

In addition, for each disclosure required to be included in a log maintained for purposes of producing such reports, each City Department will document:

a. The date of the disclosure.
b. The name of the entity or person who received the protected health information and, if known, the entity or person's address.
c. A brief description of the protected health information disclosed.
d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
e. Any written disclosure report that is provided to an individual.

29.5 ACCESS TO PROTECTED HEALTH INFORMATION. Each City Department (excluding areas that are not responsible for employee health benefit plans or billing, do not receive or transmit protected health information or do not otherwise receive individuals' complaints in the regular course of business) will document the contents of the designated record set that is subject to access by individual, and the titles of the persons or offices responsible for receiving and processing requests for access.

29.6 AMENDMENT OF PROTECTED HEALTH INFORMATION. Each City Department (excluding areas that are not responsible for employee health benefit plans or billing, do not receive or transmit protected health information or do not otherwise receive individuals' complaints in the regular course of business) will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.

29.7 RESTRICTION REQUESTS GRANTED. When a City Department agrees to honor an individual's request for a restriction on the Department's use or disclosure of protected health information for treatment, payment, insurance or health care-related operations, the Department must document the restrictions.

29.8 DISCIPLINARY ACTION FOR VIOLATIONS. Any time that disciplinary action is taken for violation of privacy and security policies or related procedures, the relevant manager or supervisor will ensure that such action is appropriately documented. At a minimum, such documentation will identify the disciplined workforce member, the date of the action, the nature of the violation, and the type of sanction imposed. In addition to documenting the action in the individual's personnel file (or in a central file, for workforce members such as volunteers for whom no personnel file is maintained), the manager or supervisor must provide such documentation without individual identification to the Privacy and Security Officer to facilitate a City Department's response to any external inquiry.

29.9 BUSINESS ASSOCIATE ASSURANCES. Each affected City Department must ensure that written assurances regarding privacy and security are obtained from that Department's business associates in accordance with the City's Administrative Policy regarding "Business Associate Contracting." These written assurances must be retained as documentation in accordance the section below titled "Retention of Documentation."

29.10 AUTHORIZATIONS FOR USE AND DISCLOSURE. Any signed authorization for use and/or disclosure of protected health information, and any written revocation of a previously

signed authorization, will be retained as documentation in accordance with this policy.

29.11 REPORTING DOCUMENTATION. Refer to the City of Green Bay Notice of Privacy Practices for policies addressing HIPAA Privacy Regulation documentation standards relating to protected health information use and reporting requirements.

29.12 RETENTION OF DOCUMENTATION. All documentation required under this policy will be retained for a period of not less than six (6) years from the date of its creation or when it was last in effect, except for logging of disclosures, which shall be retained indefinitely. Each affected City Department will implement procedures designed to ensure that affected documentation is retained for the required period of time and that it is available as necessary to comply with the requirements of the HIPAA Privacy and Security regulations (for example, in the case of documentation to enable a timely and accurate accounting in response to an individual's request), and to demonstrate compliance in connection with monitoring activities, audits and investigations.

References:

Policy Cross - Reference

Personnel Policy Ch. 3 – Records and Transaction Management
Personnel Policy Ch. 10 – Employee Assistance Program
Personnel Policy Ch. 14 – Discipline and Discharge
Personnel Policy Ch. 19 – Electronic Communications and Information System Usage Policy
Fire Department Policy [Data Privacy]
Police Department Policy [Data Privacy]
@ Business Associate Contracting
@ Responding to Privacy and Security Violations
@ Information Technology Security Incidents Management

Regulatory Reference

45 C.F.R. § 160.103
45 C.F.R. §§164.102 et seq.
Wis. Stat. §§ 146.81 et seq.

This policy, which is reviewed annually, supersedes all prior policies of the same or similar subject except to the extent it is inconsistent with the express terms of a collective bargaining or individual agreement.