City of WHITEWATER		HIPAA Privacy Policy			
Owner:	Privacy Officer	Approving Position:	Common Council	Pages:	8
Issue Date:		Revision Date:		Review Date:	
Special Instructions:	Annual review schedule				

I. Purpose

The purpose of this Privacy Policy is to ensure that the City of Whitewater, as sponsor of its self-funded health plan, protects the privacy and security of Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and applicable state laws. This Policy establishes the City's commitment to safeguarding sensitive information, outlines the permitted uses and disclosures of PHI, informs individuals of their rights, and provides guidance to workforce members in handling PHI responsibly.

II. Introduction and Legal Authority

The City of Whitewater ("the City"), as the sponsor of a self-funded group health plan ("the Plan"), is committed to compliance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E), the HIPAA Security Rule, and the HITECH Act. These laws establish national standards to protect the privacy and security of Protected Health Information ("PHI").

This Privacy Policy describes the City's policies and procedures for the use, disclosure, and safeguarding of PHI in connection with the Plan. This document is intended as a guideline for compliance with HIPAA requirements. It does not create enforceable rights for plan participants, dependents, or business associates beyond those granted under HIPAA. In the event of conflict between this Policy and HIPAA, the requirements of HIPAA shall govern.

The City reserves the right to amend or change this Privacy Policy at any time, including retroactively, subject to applicable HIPAA notice requirements.

III. Scope

This policy applies to all City employees, elected officials, contractors, and agents who have access to PHI through the administration of the self-funded health plan. It covers all forms of PHI—oral, written, or electronic.

IV. Definitions

1. Protected Health Information (PHI): Individually identifiable health information in any form (electronic, written, or oral) as defined by HIPAA.
    a. For purposes of this Privacy Policy, PHI does not include:
        1) Summary health information that is disclosed to the Plan Sponsor for the purpose of obtaining premium bids, or modifying, amending or terminating the Health Plan;
        2) Enrollment and disenrollment information for the Health Plan;
        3) PHI that is disclosed to the Health Plan or the Plan Sponsor pursuant to a valid HIPAA authorization; and
        4) Employment records that are created or received by the Plan Sponsor in its role as an employer, and not as a sponsor of the Health Plan.
2. Summary Health Information: Information that summarizes claims history, expenses, or types of claims experienced by participants, stripped of identifiers other than a five-digit ZIP code.

V. Permitted Uses and Disclosures

The Plan may use or disclose PHI only as permitted under HIPAA:

1. Treatment, Payment, and Health Care Operations (TPO): To administer claims, coordinate care, and manage plan operations.
2. As Required by Law: Disclosures required under state or federal law.
3. To Business Associates: Provided appropriate HIPAA Business Associate Agreements are in place.
4. With Authorization: Any other use/disclosure requires the individual's written authorization.

For benefits administered through third-party insurance issuers or HMOs, those entities are directly responsible for compliance with HIPAA and will issue their own Notice of Privacy Practices.

VI. Safeguards

The City implements the following safeguards to protect PHI:

1. Administrative: Designation of a Privacy Officer, workforce HIPAA training, role-based access limitations.
2. Technical: Password protection and secure transmission of PHI.
3. Physical: Restricted access, locked storage, secure disposal and shredding of PHI.

VII. Workforce Training and Sanctions

1. Training: All workforce members with PHI access receive HIPAA training appropriate to their roles.
2. Violations of this policy or HIPAA requirements may result in disciplinary action consistent with City employment policies, up to and including termination. Sanctions may range from:
    a. Verbal warning
    b. Written warning
    c. Retraining or remedial education
    d. Temporary suspension of access to PHI systems
    e. Suspension without pay
    f. Demotion
    g. Termination of employment
    h. Legal consequences (where applicable)
3. The employee subject to sanctions may request a review or appeal according to City of Whitewater procedures.

VIII. Employee Rights

1. Covered employees have the right to:
    a. Access copies of their PHI.
    b. Request corrections to their PHI.
    c. Request restrictions on uses or disclosures.
    d. Receive an accounting of non-routine disclosures.
    e. Request confidential communications.
2. Requests must be submitted in writing to the Privacy Officer.

IX. Compliance Requirements

1. No Intimidation or Retaliation: The City will not threaten, coerce, intimidate, discriminate, or retaliate against any individual for exercising HIPAA rights.
2. No Waiver of Rights: Participants cannot be required to waive HIPAA rights as a condition of enrollment or benefits.

X. Breach Notification

1. Purpose: To establish procedures for identifying, investigating, and responding to potential breaches of Protected Health Information (PHI) and to comply with the HIPAA Breach Notification Rule (45 CFR §§ 164.400–414).
2. Definition of a Breach: A breach is any acquisition, access, use, or disclosure of PHI that is not permitted under the HIPAA Privacy Rule and that compromises the security or privacy of the information. A breach excludes:
    a. Unintentional access or use of PHI by a workforce member acting in good faith within their authority.
    b. Inadvertent disclosures between authorized persons within the Plan.
    c. Disclosures where there is a good faith belief that the recipient could not reasonably retain the PHI.

3. Risk Assessment: The City will conduct a risk assessment following any impermissible use or disclosure of PHI to determine if it qualifies as a reportable breach. The assessment will consider:
   a. The nature and extent of PHI involved.
   b. The identity of the unauthorized person who used or received the PHI.
   c. Whether the PHI was actually acquired or viewed.
   d. The extent to which the risk has been mitigated.
4. Workforce Reporting
   a. All workforce members must immediately report any known or suspected breach of PHI to the Privacy Officer.
   b. Failure to report may result in disciplinary action under the City's disciplinary policy.
5. Notification Requirements
   a. Individuals: The City will notify affected individuals without unreasonable delay, but no later than 60 days after discovery of the breach.
   b. U.S. Department of Health & Human Services (HHS): If a breach affects 500 or more individuals, HHS will be notified immediately. If a breach affects fewer than 500 individuals, HHS will be notified annually.
   c. Media: If a breach affects more than 500 residents in a state or jurisdiction, the City will provide notice to prominent media outlets.
   d. All notifications will include a description of the breach, the types of information involved, steps individuals should take to protect themselves, and measures the City is taking to investigate and mitigate the breach.
6. Mitigation
   a. The City will take reasonable steps to mitigate, to the extent practicable, any harmful effects resulting from a breach.
   b. This may include retrieval of information, securing electronic systems, and offering credit monitoring where appropriate.
7. Documentation and Retention
   a. The City will document all breach investigations, risk assessments, notifications, and mitigation efforts.
   b. Records will be retained for at least six (6) years in accordance with HIPAA requirements.

XI. Privacy Officer

The Privacy Officer is responsible for the development and implementation of the Health Plan's policies and procedures relating to the privacy of PHI. The Privacy Officer will work with the Health Plan's Security Official with respect to electronic PHI (ePHI).

1. The City designates its HR Manager as the Privacy Officer responsible for:
   a. Overseeing HIPAA compliance.
   b. Responding to inquiries and complaints.
   c. Ensuring implementation of safeguards.
2. Contact Information:
   Sara Marquardt – HR Manager/Privacy Officer

City of Whitewater
262-473-1387
smarquardt@whitewater-wi.gov

XIII. Complaints

Participants may submit complaints regarding privacy practices to the Privacy Officer or directly to the U.S. Department of Health & Human Services (HHS). The City will not retaliate against individuals for filing complaints.

XIV. Policy Review and Updates

This Privacy Policy will be reviewed annually and revised as necessary to reflect changes in law, regulations, or municipal operations.

XV. Job Aids

1. Privacy Notice (Notice of Privacy Practices)

NOTICE OF PRIVACY PRACTICES

Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed by the City of Whitewater as sponsor of its self-funded health plan, and how you can access this information. Please review it carefully.

YOUR RIGHTS

You have the right to:

1. Get a copy of your health and claims records.
2. Request corrections to your health and claims records.
3. Request confidential communications (for example, to an alternate address or phone number).
4. Ask us to limit the information we share.
5. Get a list (accounting) of non-routine disclosures of your information.
6. Request and receive a copy of this privacy notice.
7. Designate someone to act for you if you have given them medical power of attorney or legal guardianship.
8. File a complaint with the privacy officer if you believe your privacy rights have been violated.
9. You may also file a complaint with the U.S. Department of Health & Human Services, Office for Civil Rights, by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/.
10. Be free from retaliation for filing a complaint.

YOUR CHOICES

You have choices in how we use and share your information in the following situations:

1. Answering questions from family members or friends involved in your benefits:
   You may choose to designate specific individuals (such as family members or friends) with whom we are permitted to share information related to your benefits. Instructions for designating individuals will be provided separately, or you may contact Human Resources to complete the appropriate form.
2. Coordinating communications in disaster relief situations:
   We may use or share limited information to help coordinate with disaster

relief organizations or relevant personnel. In most cases, this does not involve disclosing Protected Health Information (PHI).

OUR USES AND DISCLOSURES

We typically use or share your health information in the following ways:

1. Help manage your benefits.
    - We can use your health and claims information to administer your health plan.
    - *Example:* A provider sends us information about a claim so we can determine plan coverage.
2. Run our organization.
    - We use your information to operate the health plan, improve services, and contact you when necessary.
    - *Example:* We use aggregated claims information to evaluate plan performance and control costs.
3. Pay for your health services.
    - We can use and disclose your information to pay for covered health services.
    - *Example:* We share information with your dental plan to coordinate benefits.
4. Plan administration.
    - We may disclose your information to City officials who perform plan administration functions, subject to safeguards that limit access only to those who need it to perform their duties.
5. Other required uses and disclosures.
    - We may share your information when required by law, such as:
      a. Public health and safety issues (disease prevention, reporting abuse or neglect).
      b. Law enforcement or government oversight.
      c. Workers' compensation claims.
      d. Court orders, subpoenas, or other legal processes.
      e. Special government functions (e.g., national security).

OUR RESPONSIBILITIES

1. We are required by law to maintain the privacy and security of your protected health information (PHI).
2. We will notify you promptly if a breach occurs that may have compromised the privacy or security of your information.

3. We must follow the duties and privacy practices described in this notice and give you a copy upon request.
4. We will not use or share your information other than as described here unless you give us written permission. You may revoke your permission in writing at any time.
5. We will not retaliate against you for filing a complaint.

CHANGES TO THE TERMS OF THIS NOTICE

We may change the terms of this notice, and the changes will apply to all information we have about you. The revised notice will be available upon request, posted on the City's website, and mailed to you if required by law.

CONTACT INFORMATION

For more information or to file a complaint, contact:
Sara Marquardt, HR Manager/Privacy Officer
City of Whitewater
312 W Whitewater Street, Whitewater WI 53190
262-473-1387 or smarquardt@whitewater-wi.gov