

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

- 15.01 Purpose
- 15.02 Definitions
- 15.03 Security Official
- 15.04 Risk Analysis
- 15.05 Risk Management
- 15.06 Plan Document
- 15.07 Disclosures of Electronic PHI to Business Associates
- 15.08 Breach Notification Requirements
- 15.09 Documentation

15.01 Purpose

- 15.01.01 The City of Tumwater (the City) sponsors and self-administers a group health plan (Health Care Flexible Spending Account program) (the Plan). Members of the City's workforce may create, receive, maintain, or transmit electronic protected health information (as defined below) on behalf of the City, for Plan administration functions. The Plan may also have one or more business associates that perform functions for the Plan.
- 15.01.02 The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and their implementing regulations and guidance require the Plan to implement various security measures with respect to electronic protected health information (electronic PHI).
- 15.01.03 It is the Plan's policy to comply fully with HIPAA's security regulations.
- 15.01.04 No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan. This Policy does not address requirements under federal laws other than HIPAA or under state laws.

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.02 Definitions

- 15.02.01 “Business Associate” - an entity (other than the City) that:
- a) Performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
 - b) Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.
- 15.02.02 “Electronic Media” -
- a) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
 - b) Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.
- 15.02.03 “Electronic Protected Health Information” - Protected health information that is transmitted by or maintained in electronic media.
- 15.02.04 “Employee” - includes individuals such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the City, whether or not they are paid by the City.
- 15.02.05 “Protected Health Information (PHI)” - the information that is subject to and defined in the Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to in this Policy as “Exempt Information”:

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.02 Definitions

- a) summary health information, as defined by HIPAA's privacy rules, for purposes of (1) obtaining premium bids or (2) modifying, amending, or terminating the Plan;
- b) enrollment and disenrollment information concerning the Plan which does not include any substantial clinical information; or
- c) PHI disclosed to the Plan under a signed authorization that meets the requirements of the HIPAA privacy rules.

15.03 Security Official

The Information Technology Manager is the Security Official for the Plan. The Security Official is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy.

15.04 Risk Analysis

15.04.01 The Plan has no employees. All of the Plan's functions, including creation and maintenance of its records, are carried out by employees of the City and/or by business associates of the Plan. The Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the City and business associates. Accordingly, the City and/or business associates create and maintain all of the electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and controls their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan. That ability lies solely with the City and business associates.

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.04 Risk Analysis

15.04.02 Because the Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the City and business associates affecting the security of Plan electronic PHI, and the City and business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administration functions for the Plan, the Plan's policies, and procedures, including this Policy, do not address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 CFR Part 164:

- a) security management process;
- b) workforce security;
- c) information access management;
- d) security awareness and training;
- e) security incident procedures;
- f) contingency plan;
- g) evaluation;
- h) facility access controls;
- i) workstation use;
- j) workstation security;
- k) device and media controls;
- l) access control;
- m) audit controls;
- n) integrity;
- o) person or entity authentication; and
- p) transmission security.

15.05 Risk Management

- a) The Plan manages risks to its electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account, the following:
 - 1) the size, complexity, and capabilities of the Plan;
 - 2) the Plan's technical infrastructure, hardware, software, and security capabilities;
 - 3) the costs of security measures, and
 - 4) the criticality of the electronic PHI potentially affected.

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.05 Risk Management

- b) Based on risk analysis discussed in section 15.04, the Plan made a reasoned and well-informed and good-faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures set forth herein and the measures of the City, and other business associates, to reduce risks to the confidentiality, integrity and availability of electronic PHI.

15.06 Plan Document

The Plan document shall include provisions requiring the City to:

- a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the City creates, receives, maintains, or transmits on behalf of the Plan (the Plan electronic PHI);
- b) ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the City (which were adopted as described in the Plan's privacy policy);
- c) ensure that any agents or subcontractors to whom the City provides Plan electronic PHI agree to implement reasonable and appropriate security measures to protect the Plan electronic PHI; and
- d) report to the Security Official any security incident of which the City becomes aware.

15.07 Disclosures of Electronic PHI to Business Associates

The Plan may permit one or more business associates to create, receive, maintain, or transmit electronic PHI on its behalf only if the Plan first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

- a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Plan (the Contract electronic PHI);

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.07 Disclosures of Electronic PHI to Business Associates

- b) ensure that any agents or subcontractors to whom the business associate provides Contract electronic PHI agree to implement reasonable and appropriate security measures to protect the Contract electronic PHI;
- c) report to the Plan any security incident of which the business associate becomes aware;
- d) take required steps with respect to breach notification requirements, and
- e) authorize termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.

15.08 Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification, when required, to affected individuals, HHS, and the media (when required) if the Trust learns of a breach of unsecured PHI.

15.09 Documentation

- 15.09.01 The Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Plan electronic PHI, and any changes to policies or procedures will be documented promptly.
- 15.09.02 Except to the extent that they are carried out by the City or business associates, the Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this policy, for example).
- 15.09.03 Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

CITY OF TUMWATER
POLICY MANUAL - PART 2: OPERATING POLICIES

SECTION 15
HIPAA SECURITY

15.09 Documentation

- 15.09.04 The Plan will make its policies, procedures, and other documentation available to the Security Official and the City, as well as business associates or other persons responsible for implementing the procedures to which the documentation pertains.