CITY OF BREMERTON HUMAN RESOURCES POLICY	HIPAA Privacy Compliance	
INDEX Human Resources Compliance 3-20-13	EFFECTIVE DATE: 01/22/15 REVIEW DATE:	APPROVED

REFERENCE

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HITECH)

PURPOSE

The purpose of this policy is to implement the relevant privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the regulations promulgated thereunder. This policy shall apply to all City divisions and departments.

DEFINITIONS

"Business Associate" means an entity that assists another entity covered by HIPAA to perform a function or activity regulated by HIPAA's administrative simplification mandates or that provides certain services (for example, legal or consulting services) involving the use or disclosure of individually identifiable health information.

"Health Insurance Portability and Accountability Act of 1996 (HIPAA)" means a federal law, enacted in 1996, that made comprehensive changes to the portability of health insurance and established privacy rules. Pub.L.No. 104-191 (August 1996).

"Health Information Technology for Economic and Clinical Health Act (HITECH)" enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

"Participant" means an employee or former employee who is or may become eligible to receive a benefit from a plan.

"Privacy Officer" means the person designated by the employer or health care entity to monitor the entity's privacy responsibilities and to resolve complaints filed participants regarding privacy issues.

"Protected Health Information" (PHI) and/or "Electronic Protected Health Information" (ePHI) also referred to as "Personal Health Information" means individually identifiable health information that is maintained or transmitted in

any form by any entity covered by HIPAA, such as health plans and most health care providers.

POLICY

It is the policy of the City that specific individuals within the City's workforce are assigned the responsibility of implementing and maintaining the Health Insurance Portability and Accountability Act (HIPAA) privacy requirements. Furthermore, these individuals will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum there will be one individual designated by the Mayor as the City's Privacy Officer.

The Privacy Officer in conjunction with the appropriate administrative departments, shall:

- prepare consent/authorization forms consistent with HIPAA;
- prepare and distribute privacy notices to participants about the use and disclosures of protected health information;
- review the process for storing information to allow for the tracking of disclosures and accessing of participant records;
- train employees having access to protected health information and maintain records of the training; and

Uses and Disclosures of PHI and/or ePHI

PHI and/or ePHI may not be used or disclosed except when at least one of the following conditions is true. Attachment A attached hereto may be used as a guide to establishing protocols related to use and disclosure of PHI and ePHI.

a. The individual who is the subject of the information has authorized use or disclosure.
b. The individual who is the subject of the information has received an appropriate Notice of Privacy Practices (or if a dependent, the named insured has received Notice), thus allowing the use or disclosure. The use or disclosure is for treatment, payment, or health care operations.
c. The individual who is the subject of the information agrees or does not object to the disclosure and the disclosure is to persons involved in the health care of the individual.
d. The disclosure is to the individual who is the subject of the information or to the U.S. Department of Health and Human Services for compliance-related purposes.
e. The use or disclosure is for one of the HIPAA "public purposes" (i.e. required by law; determination of benefits under the FMLA, ADA, workers compensation leave, and other disability claims; etc.)

Security Safeguards

Attachment A attached hereto may be used as a guide for conducting an assessment related to establishing the following security safeguards for PHI and ePHI.

1) **Administrative Safeguards.**

Access to PHI and/or ePHI is limited to certain employees. The following employees/retirees have access to PHI and ePHI:

Human Resources Employees
Risk Manager
Payroll Specialist
Accounting Assistants
(Processing Claims - Finance Department)
Safety Committee
Information Services Employees
All Fire Department Employees
City Clerk
Members of LEOFF I Pension Boards
City Auditor

It is the City's policy to ensure that all members of its workforce and LEOFF I Pension Boards who have access to PHI and/or ePHI receive the necessary and appropriate training to permit them to carry out their functions in compliance with HIPAA.

a) Security Management Process - Risk Analysis (required): Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated.
b) Security Management Process - Risk Management (required): Implement sufficient measures to reduce these risks to an appropriate level.
c) Security Management Process - Sanction Policy (required): Implement sanction policies for employees who fail to comply.
d) Security Management Process - Information Systems Activity Reviews (required): Regularly review system activity, logs, audit trails, etc.
e) Assigned Security Responsibility - Officers (required): Designate HIPAA Security and Privacy Officers.
f) Workforce Security - Employee Oversight (addressable): Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment.
g) Information Access Management - Multiple Organizations (required): Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access.
h) Information Access Management - ePHI Access (addressable): Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI.
i) Security Awareness and Training - Security Reminders (addressable): Periodically send updates and reminders about security and privacy policies to employees.
j) Security Awareness and Training - Protection Against Malware (addressable): Have procedures for guarding against, detecting, and reporting malicious software.
k) Security Awareness and Training - Login Monitoring (addressable): Institute monitoring of logins to systems and reporting of discrepancies.
l) Security Awareness and Training - Password Management (addressable): Ensure that there are procedures for creating, changing, and protecting passwords.
m) Security Incident Procedures - Response and Reporting (required): Identify, document, and respond to security incidents.

n) Contingency Plan - Contingency Plans (required): Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data.
o) Contingency Plan - Contingency Plans Updates and Analysis (addressable): Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.
p) Contingency Plan - Emergency Mode (required): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
q) Evaluations (required): Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures.
r) Business Associate Agreements (required): Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Choose partners that have similar agreements with any of their partners to which they are also extending access.

2) Physical Safeguards

a) Physical documents containing PHI will be stored in designated secure locations and in files designated as "confidential."
b) Facility Access Controls - Contingency Operations: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
c) Facility Access Controls - Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
d) Facility Access Controls - Access Control and Validation Procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
e) Facility Access Controls - Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g. hardware, walls, doors, and locks).
f) Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.
g) Workstation Security: Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
h) Device and Media Controls - Disposal: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
i) Device and Media Controls - Media Re-Use: Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

j) Device and Media Controls - Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
k) Device and Media Controls - Data Backup and Storage: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

3) Technical Safeguards and Access Control

Technical safeguards will be implemented using current technology solutions together with the policy and procedures for its use to protect electronic protected health information and control access to it. This will include but not limited to the use of encryption, routers, firewalls, and switches with VLANs / port security. Information Services will ensure that only authorized employees will have access to protected health information, and that they will have access to only the minimum amount of protected information necessary for them to perform the functions of their position.

a) Unique User Identification: Users will be assigned unique name and/or number for identifying and tracking user identity to all systems that contain ePHI.
b) Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
c) Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
d) Encryption and Decryption: Identify and implement a mechanism to encrypt and decrypt ePHI where deemed appropriate.
e) Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
f) Integrity - Mechanism to Authenticate ePHI: Identify and Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner whenever deemed appropriate.
g) Authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
h) Transmission Security - Integrity Controls: Evaluate and implement whenever deemed appropriate, security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
i) Transmission Security – Encryption: Evaluate and implement whenever deemed appropriate a mechanism to encrypt ePHI.

Complaint Procedure

All complaints relating to the protection of health information shall be investigated and resolved in a timely fashion. All complaints will be addressed to the Privacy Officer who will be duly authorized to investigate complaints and implement resolutions if the complaint stems from a valid are of non-compliance with HIPAA Privacy Rule. The effects of any unauthorized use or disclosure of protected health information shall be mitigated to the extent possible.

No employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA.

A complainant is encouraged to use the following procedure to resolve complaints of violation of privacy pertaining to private health information under HIPAA regulations.

a) The complainant must inform the Privacy Officer(s) for the City of Bremerton immediately when there is an allegation of violation of disclosure of private health information under this policy. Complaints should be filed with the Human Resources Manager for distribution to the appropriate Privacy Officer.

b) The following information in support of the allegation must be provided in writing and must include the following:

    1. Name of the complainant;
    2. Date and time of the complaint
    3. Basic facts describing the nature of the alleged violation
    4. Name of the staff member who received the complaint.

c) The Privacy Officer shall provide a written response to the complainant pertaining to the resolution of the complaint within thirty days of receipt of the complaint.
d) If the complainant is not satisfied with the resolution of the complaint, an appeal of the Privacy Officer's decision may be filed with the office of the Mayor. The appeal must be filed within fifteen days of the employee's receipt of the Privacy Officer's written response.
e) The Mayor shall respond in writing to the complainant within fifteen days of receipt of the appeal.
f) If the complainant is not satisfied with the response from the Mayor, he/she may also file a complaint with the Secretary of the U.S. Department of Health and Human Services at 1-877-696-6775.

The complaint procedure shall not rescind any procedures available under any existing federal or state law. All employees are encouraged to use the internal complaint procedure whenever it is believed that a violation has occurred.

Employees are required to cooperate fully in processing of the complaint. Employees will be allowed to have a representative of their choice, including legal counsel or a union representative, present at or during any investigatory meeting.

An employee who files a complaint that the employee knows to be false will be disciplined, up to and including termination, for filing a false complaint. Sanctions for using or disclosing protected health information in violation of this policy will include discipline up to and including termination.

ATTACHMENTS

Attachment A HIPAA PRIVACY CHECKLIST
Attachment B HIPAA SECURITY CHECKLIST
Notice of Privacy Practices

ATTACHMENT A

HIPAA Privacy Checklist

The following summarizes required and recommended privacy policies and forms per the HIPAA Privacy Rule. The citations are to 45 CFR Part 164. The Privacy Rule is subject to periodic amendment. Users should review the current rule requirements to ensure continued compliance.

Policies		
HIPAA Privacy Rule Reference	**Policy**	**Status (Complete, N/A)**
USE AND DISCLOSURE: GENERAL RULES		
164.506	Consent is implied for treatment, payment and health care operations; no written authorization is required except for psychotherapy notes.	
164.510	Providing notice and chance for patient to agree or object is sufficient for certain disclosures, including disclosures to family members or others involved in the patient's care; for facility directories; and to provide notice in emergency situations.	
164.512	Certain disclosures may be made per regulatory exceptions subject to specific conditions, e.g., uses or disclosures required by law; to avert a serious and imminent health; for public health activities; in response to a court order or subpoena; to law enforcement, etc.	
164.508	Authorizations are generally required for all other uses or disclosures, including uses or disclosures of psychotherapy notes; for most marketing activities; sale of protected health information; etc. Include the elements for a valid authorization.	
USE AND DISCLOSURE: SPECIAL RULES		
164.514(f)	Fund raising uses or disclosures generally require authorization except in limited circumstances.	
164.512(i)	Research generally requires authorization unless certain conditions are met.	
164.502(f)	Privacy protection continues after death for a period of 50 years.	
164.502(g)	Personal representatives and parents of unemancipated minors are generally entitled to access information and exercise other patient rights, subject to certain exceptions.	
164.514(h)	Covered entities should verify a requesting person's identity and authority before disclosing information.	
164.502(d); 164.514(e)	Covered entities may "de-identify" information, thereby avoiding HIPAA restrictions.	
164.530(c)	Safeguards for facsimiles, e-mails, and telephone communications may be appropriate. (Not expressly required by privacy regulations, but may help satisfy safeguards per 164.530(c))	
MINIMUM NECESSARY STANDARD		
164.502(b)	Limit use or disclosure to the minimum necessary to accomplish the purpose, subject to specified situations.	
164.514(d)	Define and limit workforce members' access to protected information.	
164.514(d)	Establish protocols for routine disclosures, and processes for handling others on an individual basis.	
164.514(d)	Establish protocols for routine requests for information, and processes for handling others on an individual basis.	

64.514(d)	Do not request entire record if not necessary.	
PATIENT RIGHTS		
164.522(a)	Right to request additional restrictions on use or disclosure for treatment, payment or health care operations; however, the provider is not obligated to agree to restrictions except in limited situation.	
164.522(b)	Right to request alternative means or location of communications, including process for requesting alternatives and limitations on requests.	
164.524	Right to access protected health information, including process for requesting access; time limits and process for responding; bases for denials; and determination of reasonable costs.	
164.526	Right to amend protected health info, including process for requesting amendments; time limits and process for responding; bases and process for denials; attaching amendments or requests; and notifying others about requests.	
164.528	Right to request accounting of protected health information, including process for capturing information for accounting; process for requesting accounting; time limits and process for responding; and limitations on requests.	
NOTICE OF PRIVACY PRACTICES		
164.520	Provision and posting of notice.	
164.520	Good faith efforts to obtain acknowledgment.	
BUSINESS ASSOCIATES		
164.502(e) 164.504(e)	Process for obtaining business associate contracts; taking action for violations; and obtaining information from business associates to comply with provider's responsibilities.	
NOTIFICATION REQUIREMENTS FOR BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION		
164.402	Identifying when a breach occurs.	
164.402	Securing protected health information.	
164.404	Notice to individuals, including timing, content, and providing substitute notice.	
164.408	Notice to HHS, including annual and immediate notices to HHS, timing, and content. The HHS electronic reporting process may be accessed through the OCR's HIPAA website, http://www.hhs.gov/ocr/privacy/.	
164.406	Notice to the media, including form, timing and content.	
164.410	Notice by business associates, including timing and required information.	
164.412	Delay in notice at request of law enforcement.	
ADMINISTRATIVE REQUIREMENTS		
164.530(a)	Designation of privacy offer and contact person.	

ATTACHMENT A

164.530(b)	Training existing and new members of the workforce.	
164.530(c)	Use of technical, administrative, and physical safeguards to avoid improper or incidental disclosures.	
164.530(e)	Sanctions against workforce members for violation of policies and regulations.	
164.530(d)	Patient complaints, including the process for complaining and responding to complaints.	
164.530(f)	Mitigation of improper disclosures.	
160.410	Correction of any violations within 30 days to avoid penalties.	
164.530(g)	No retaliation or intimidation against patients or others who exercise HIPAA rights.	
164.530(h)	No conditioning treatment on a waiver of HIPAA rights.	
164.530(i)	Document retention, including identifying documents that must be retained and period of retention.	
Forms		
HIPAA Privacy Rule Reference	**Form**	**Status (Complete, N/A)**
164.520	Notice of privacy practices.	
164.520	Acknowledgment of receipt of privacy practices.	
164.504(e)	Business associate contract.	
164.514(e)	Data use agreement (if used).	
USE AND DISCLOSURE FORMS		
164.508(c)	Authorization	
164.510	Objection to disclosure per 164.510.	
164.514(f)	Opt-out of fundraising.	
PATIENT RIGHTS FORMS		
164.522(a)	Request for additional restrictions on use or disclosure / denial of request. ☐ Notice of denial of request.	
164.522(b)	Request for alternative means or location for communication / action on request. ☐ Notice of denial of request.	
164.524; 164.524(d)	Request for access to information / action on request. ☐ Notice of denial of request.	
164.526 164.526(d)	Request for amendment of information / action on request. ☐ Notice of denial of request.	
164.528 164.528(b) 164.528	Request for accounting of information / action on request. ☐ Accounting log. ☐ Notice of denial of request.	

ATTACHMENT A

ADMINISTRATIVE REQUIREMENTS		
164.530(a)	Privacy officer designation.	
164.530(a)	Contact officer designation.	
164.530(b)	Employee training certification.	
164.530(d)	Complaint form / action on complaint.	
164.530(f)	Privacy violation report form / action in response to incident (including documentation of sanctions).	
164.408	Log of breaches reportable to HHS on annual basis.	

ATTACHMENT B

HIPAA Security Checklist

The following checklist summarizes HIPAA Security Rule requirements that should be implemented by covered entities and business associates. The citations are to 45 CFR § 164.300 et seq. The Security Rule is subject to periodic amendment. Users should review the current rule requirements on a regular basis to ensure continued compliance.

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete Date or N/A
ADMINISTRATIVE SAFEGUARDS		
164.308(a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(A)	Risk Analysis: Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated. (R)	
164.308(a)(1)(ii)(B)	Risk Management: Implement sufficient measures to reduce these risks to an appropriate level. (R)	
164.308(a)(1)(ii)(C)	Sanction Policy: Implement sanction policies for employees who fail to comply. (R)	
164.308(a)(1)(ii)(D)	Information Systems Activity Review: Regularly review system activity , logs, audit trails, etc. (R)	
164.308(a)(2)	Officers: Designate HIPAA Security and Privacy Officers (R)	
164.308(a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).	
164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C)	Employee Oversight: Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment. (A)	
164.308(a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(A)	Multiple Organizations: Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access. (R)	
164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C)	Implement policies and procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI. (A)	
164.308(a)(5)(i)	Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management).	
164.308(a)(5)(ii)(A)	Security Reminders: Periodically send updates and reminders about security and privacy policies to employees. (A)	
164.308(a)(5)(ii)(B)	Protection Against Malware: Implement procedures for guarding against, detecting, and reporting malicious software. (A)	
164.308(a)(5)(ii(C)	Login Monitoring: Institute monitoring of logins to systems and reporting of discrepancies. (A)	

164.308(a)(5)(ii)(D)	Password Management: Ensure that there are procedures for creating, changing, and protecting passwords. (A)	
164.308(a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	Response and Reporting: Identify, document and respond to security incidents (R)	
164.308(a)(7)(i)	**Contingency plan:** Ensure that there are accessible backups of ePHI and that there are procedures to restore lost data.	
164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B)	Ensure that there are accessible backups of ePHI and that there are procedures for restoring any lost data. (R)	
164.308(a)(7)(ii)(C)	Emergency Mode: Establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. (R)	
164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E)	Contingency Plans Updates and Analysis: Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components. (A)	
164.308(a)(8)	**Evaluations:** Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures (R)	
164.308(b)(1) 164.308(b)(4)	**Business associate contracts and other arrangements:** Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Chose partners that have similar agreements with any of their partners to which they are also extending access. (R)	
PHYSCIAL SAFEGUARDS		
164.310(a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.	
164.310(a)(2)(i)	Contingency Operations: Establish (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency (A)	
164.310(a)(2)(ii)	Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. (A)	
164.310(a)(2)(iii)	Access Control and Validation Procedures: Implement procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision. (A)	
164.310(a)(2)(iv)	Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). (A)	
164.310(b)	**Workstation Use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI (R)	

164.310(c)	**Workstation Security:** Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. (R)	
164.310(d)(1)	**Device and media controls:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	
164.310(d)(2)(i)	Disposal: Implement policies and procedures to address final disposition of ePHI, and/or hardware or electronic media on which it is stored. (R)	
164.310(d)(2)(ii)	Media Re-Use: Implement procedures for removal of EPHI from electronic media before the media are available for reuse. (R)	
164.310(d)(2)(iii)	Accountability: Maintain a record of the movements of hardware and electronic media and the person responsible for its movement. (A)	
164.310(d)(2)(iv)	Data Backup and Storage: Create a retrievable, exact copy of ePHI, when needed, before moving equipment? (A)	
TECHNICAL SAFEGUARDS		
164.312(a)(1)	**Access controls:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity. (R)	
164.312(a)(2)(ii)	Emergency Access Procedure: Establish (and implemented as needed) procedures for obtaining necessary ePHI during an emergency. (R)	
164.312(a)(2)(iii)	Automatic Logoff: Implement procedures that terminate an electronic session after a predetermined time of inactivity. (A)	
164.312(a)(2)(iv)	Encryption and Decryption: Implement a mechanism to encrypt and decrypt ePHI. (A)	
164.312(b)	**Audit Controls:** Implement audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. (R)	
164.312(c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	
164.312(c)(2)	Mechanism to Authenticate ePHI: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	**Person or Entity Authentication:** Implement person or entity authentication procedures to verify a person or entity seeking access ePHI is the one claimed. (R)	
164.312(e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Integrity Controls: Implement security measures to ensure electronically transmitted ePHI is not improperly modified without detection until disposed of. (A)	
164.312(e)(2)(ii)	Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate. (A)	

City of Bremerton
Notice of Privacy Practices

IMPORTANT: THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

City of Bremerton is committed to protecting your personal health information. We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as "protected health information" or "PHI." We are also required by law to provide you with the attached detailed Notice of Privacy Practices ("Notice") explaining our legal duties and privacy practices with respect to your PHI.

We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times.

PLEASE READ THE ATTACHED DETAILED NOTICE. IF YOU HAVE ANY QUESTIONS ABOUT IT, PLEASE CONTACT CHARLOTTE BELMORE, OUR HIPAA COMPLIANCE OFFICER, AT 360-473-5926 or charlotte.belmore@ci.bremerton.wa.us.

Detailed Notice of Privacy Practices

Purpose of This Notice: This Notice describes your legal rights, advises you of our privacy practices, and lets you know how City of Bremerton is permitted to use and disclose PHI about you.

Uses and Disclosures of Your PHI We Can Make Without Your Authorization
City of Bremerton may use or disclose your PHI *without* your authorization, and *without* providing you with an opportunity to object, for the following purposes:

Treatment. This includes such things as verbal and written information that we obtain about you and use pertaining to your medical condition and treatment provided to you by us and other medical personnel (including doctors and nurses who give orders to allow us to provide treatment to you). It also includes information we give to other healthcare personnel to whom we transfer your care and treatment, and includes transfer of PHI via radio or telephone to the hospital or dispatch center as well as providing the hospital with a copy of the written record we create in the course of providing you with treatment and transport. This PHI may be used or disclosed to the extent a recipient needs to know the information or to the extent necessary to provide health care to the patient.

Payment. This includes any activities we must undertake in order to get reimbursed for the services that we provide to you, including such things as organizing your PHI, submitting bills to insurance companies (either directly or through a third party billing company), managing billed claims for services rendered, performing medical necessity determinations and reviews, performing utilization reviews, and collecting outstanding accounts. This PHI may be used or disclosed to the extent a recipient needs to know the information.

Healthcare Operations. This includes quality assurance activities, licensing, and training programs to ensure that our personnel meet our standards of care and follow established policies and procedures, obtaining legal and financial services, conducting business planning, processing grievances and complaints, creating reports that do not individually identify you for data collection purposes, fundraising, and certain marketing activities. This PHI may be used or disclosed to the extent a recipient needs to know the information.

Fundraising. We may contact you when we are in the process of raising funds for City of Bremerton, or to provide you with information about our annual subscription program.

In addition, we may use your PHI for certain fundraising activities. For example, we may use PHI that we collect about you, such as your name, home address, phone number or other information, in order to contact you to raise funds for our agency. We may also share this information with another organization that may contact you to raise money on our behalf. If City of Bremerton does use your PHI to conduct fundraising activities, you have the right to opt out of receiving such fundraising communications from City of Bremerton. If you do not want to be contacted for our fundraising efforts, you should contact our HIPAA Compliance Officer, in

writing, by phone, or by email. Contact information for our HIPAA Compliance Officer(s) is listed at the end of this Notice. We will also remind you of this right to opt out of receiving future fundraising communications every time that we use your PHI to conduct fundraising and contact you to raise funds. City of Bremerton will not condition the provision of medical care on your willingness, or non-willingness, to receive fundraising communications.

Disclosure among Health Insurance Plan and Sponsor. Insofar as the City is the sponsor of your health plan, we may obtain and use certain PHI from your group health plan, health insurance issuer or HMO.

Disclosure as Health Plan. Insofar as the City is your health plan, and PHI is used or disclosed for underwriting purposes, we are prohibited from using or disclosing PHI that is genetic information for underwriting purposes.

Other Uses and Disclosure of Your PHI We Can Make Without Authorization.
City of Bremerton is also permitted to use or disclose your PHI *without* your written authorization in situations including:

- For the treatment activities of another healthcare provider we believe is providing you health care, to the extent the recipient needs to know the information;
- To another healthcare provider or entity for the payment activities of the provider or entity that receives the information (such as your hospital or insurance company);
- To another healthcare provider (such as the hospital to which you are transported) for certain healthcare operations activities of the entity that receives the information as long as the entity receiving the information has or has had a relationship with you and the PHI pertains to that relationship;
- For healthcare fraud and abuse detection or for activities related to compliance with the law;
- To a family member, other relative, or close personal friend or other individual involved in your care if we obtain your verbal agreement to do so or if we give you an opportunity to object to such a disclosure and you do not raise an objection. We may also disclose health information to your family, relatives, or friends if we infer from the circumstances that you would not object. For example, we may assume that you agree to our disclosure of your personal health information to your spouse when your spouse has called the ambulance for you. In situations where you are incapable of objecting (because you are not present or due to your incapacity or medical emergency), we may, in our professional judgment, determine that a disclosure to your family member, relative, or friend is in your best interest. In that situation, we will disclose only health information relevant to that person's involvement in your care. For example, we may inform the person who accompanied you in the ambulance that you have certain symptoms and we may give that person an update on your vital signs and treatment that is being administered by our ambulance crew;
- To a public health authority in certain situations (such as reporting a birth, death or disease, as required by law), as part of a public health investigation, to report child or

adult abuse, neglect or domestic violence, to report adverse events such as product defects under the jurisdiction of the FDA, or to notify a person about exposure to a possible communicable disease, as required by law;

- For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the healthcare system;
- For judicial and administrative proceedings, as required by a court or administrative order, or in some cases in response to a subpoena or other legal process;
- For law enforcement activities in limited situations, such as when there is a warrant for the request, or when the information is needed to locate a suspect or stop a crime;
- For military, national defense and security and other special government functions;
- To avert a serious threat to the health and safety of a person or the public at large to the extent a recipient needs to know the information;
- For workers' compensation purposes, and in compliance with workers' compensation laws;
- To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law;
- If you are an organ donor, we may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation, or to an organ donation bank, as necessary to facilitate organ donation and transplantation; and
- For research projects, but this will be subject to strict oversight and approvals and health information will be released only when there is a minimal risk to your privacy and adequate safeguards are in place in accordance with the law.

Uses and Disclosures of Your PHI That Require Your Written Consent

Any other use or disclosure of PHI, other than those listed above, will only be made with your written authorization (the authorization must specifically identify the information we seek to use or disclose, as well as when and how we seek to use or disclose it). Specifically, we must obtain your written authorization before using or disclosing your: (a) psychotherapy notes, other than for the purpose of carrying out our own treatment, payment or health care operations purposes, (b) PHI for marketing when we receive payment to make a marketing communication; or (c) PHI when engaging in a sale of your PHI. **You may revoke your authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that authorization.**

Uses and Disclosures of Your PHI That Require Your Written Consent

Some types of health information have greater protection under Washington State or federal laws. When required by law we will obtain your authorization before releasing HIV-related and sexually transmitted disease information that is protected by Washington State laws; alcohol and substance abuse treatment information that is protected under both Washington State and federal laws; and mental health information that is protected under both Washington State and federal laws.

Your Rights Regarding Your PHI

As a patient, you have a number of rights with respect to your PHI, including:

Right to access, copy or inspect your PHI. You have the right to inspect and copy most of the medical information that we collect and maintain about you. Requests for access to your PHI should be made in writing to our HIPAA Compliance Officer. In limited circumstances, we may deny you access to your medical information, and you may appeal certain types of denials. We have available forms to request access to your PHI, and we will provide a written response if we deny you access and let you know your appeal rights. If you wish to inspect and copy your medical information, you should contact our HIPAA Compliance Officer.

We will normally provide you with access to this information within 15 working days of your written request. If we maintain your medical information in electronic format, then you have a right to obtain a copy of that information in an electronic format. In addition, if you request that we transmit a copy of your PHI directly to another person, we will do so provided your request is in writing, signed by you (or your representative), and you clearly identify the designated person and where to send the copy of your PHI.

We may also charge you a reasonable cost-based fee for providing you access to your PHI, subject to the limits of applicable state law.

Right to request an amendment of your PHI. You have the right to ask us to amend protected health information that we maintain about you. Requests for amendments to your PHI should be made in writing and you should contact, our HIPAA Compliance Officer if you wish to make a request for amendment and fill out an amendment request form.

When required by law to do so, we will amend your information within 10 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical information in certain circumstances, such as when we believe that the information you have asked us to amend is correct.

Right to request an accounting of uses and disclosures of your PHI. You may request an accounting from us of disclosures of your medical information. If you wish to request an accounting of disclosures of your PHI that are subject to the accounting requirement, you should contact our HIPAA Compliance Officer and make a request in writing.

You have the right to receive an accounting of certain disclosures of your PHI made within six (6) years immediately preceding your request. But, we are not required to provide you with an accounting of disclosures of your PHI: (a) for purposes of treatment, payment, or healthcare operations; (b) for disclosures that you expressly authorized; (c) disclosures made to you, your family or friends, or (d) for disclosures made for law enforcement or certain other governmental purposes.

Right to request restrictions on uses and disclosures of your PHI. You have the right to request that we restrict how we use and disclose your medical information for treatment, payment or healthcare operations purposes, or to restrict the information that is provided to family, friends and other individuals involved in your healthcare. However, we are only required to abide by a requested restriction under limited circumstances, and it is generally our policy that we will not agree to any restrictions unless required by law to do so. If you wish to request a restriction on the use or disclosure of your PHI, you should contact our HIPAA Compliance Officer and make a request in writing.

City of Bremerton is required to abide by a requested restriction when you ask that we not release PHI to your health plan (insurer) about a service for which you (or someone on your behalf) have paid City of Bremerton in full. We are also required to abide by any restrictions that we agree to. Notwithstanding, if you request a restriction that we agree to, and the information you asked us to restrict is needed to provide you with emergency treatment, then we may disclose the PHI to a healthcare provider to provide you with emergency treatment.

A restriction may be terminated if you agree to or request the termination. Most current restrictions may also be terminated by City of Bremerton as long we notify you. If so, PHI that is created or received after the restriction is terminated is no longer subject to the restriction. But, PHI that was restricted prior to the notice to you voiding the restriction must continue to be treated as restricted PHI.

Right to notice of a breach of unsecured protected health information. If we discover that there has been a breach of your unsecured PHI, we are required by law to notify you about that breach by first-class mail dispatched to the most recent address that we have on file. If you prefer to be notified about breaches by electronic mail, please contact, our HIPAA Compliance Officer, to make City of Bremerton aware of this preference and to provide a valid email address to send the electronic notice. You may withdraw your agreement to receive notice by email at any time by contacting Compliance Name.

Right to request confidential communications. You have the right to request that we send your PHI to an alternate location (*e.g.,* somewhere other than your home address) or in a specific manner (*e.g.,* by email rather than regular mail). However, we will only comply with reasonable requests when required by law to do so. If you wish to request that we communicate PHI to a specific location or in a specific format, you should contact our HIPAA Compliance Officer and make a request in writing.

Internet, Email and the Right to Obtain Copy of Paper Notice

If we maintain a web site, we will prominently post a copy of this Notice on our web site and make the Notice available electronically through the web site. If you allow us, we will forward you this Notice by electronic mail instead of on paper and you may always request a paper copy of the Notice.

Revisions to the Notice

City of Bremerton is required to abide by the terms of the version of this Notice currently in effect. However, City of Bremerton reserves the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all PHI that we maintain. Any material changes to the Notice will be promptly posted in our facilities and on our web site, if we maintain one. You can get a copy of the latest version of this Notice by contacting our HIPAA Compliance Officer.

Your Legal Rights and Complaints

You also have the right to complain to us, or to the Secretary of the United States Department of Health and Human Services, if you believe that your privacy rights have been violated. You will not be retaliated against in any way for filing a complaint with us or to the government.

Should you have any questions, comments or complaints, you may direct all inquiries to our HIPAA Compliance Officer. Individuals will not be retaliated against for filing a complaint.

If you have any questions or if you wish to file a complaint or exercise any rights listed in this Notice, please contact:

Fire Department Requests
Doug Baier
Medical Officer-Captain
Bremerton Fire Department
911 Park Avenue
Bremerton, WA 98337
360-473-5380
doug.baier@ci.bremerton.wa.us

All Non-Fire Department Related Requests
Charlotte Belmore
Human Resources Manager
City of Bremerton
345 6th Street, Suite 600
Bremerton, WA 98337
360-473-5926
charlotte.belmore@ci.bremerton.wa.us

Effective Date of the Notice:

I certify that have received a copy of the City of Bremerton's Notice of Privacy Practices.

Name _____
(Please Print)

Signature _____ Date: _____