SUBJECT: PROTECTING MEDICAL INFORMATION

Division: Emergency Medical Services
Reviewed: 12-14-2017
Certified: 1-15-2018

POLICY: While providing services to community members, Clackamas Fire District #1 (CFD1) personnel are required to access, receive, maintain, transmit, or use protected health information (PHI). This policy ensures that PHI is protected, and to assure that District is compliant with the privacy laws. This policy applies to the entire District.

PHI is defined as individually identifiable health information that is maintained or transmitted in any form or medium and that relates to the past, present, or future physical or mental health condition of a patient. Confidentiality of medical records is a prime concern to the District. This directive identifies the means in which the organization protects this sensitive information.

It is the policy of the District that specific individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA privacy requirements and at a minimum the policy requires that there will be one individual or job description designated as the Privacy Officer. The District has designated the EMS Chief as the HIPAA Privacy Officer.

This policy applies to all District employees, volunteers, and interns.

PROCEDURE:

I. Definitions:

- **A. EMS Field Care Form:** This form is used to document patient information while on scene and is not intended to be a medical record.
- **B. Patient Care Form:** This form is used to document Clackamas County EMS patient information which becomes part of the patient's medical record.
- **C. Information Form:** This form was created by the Tri-County Protocol Committee and is used to convey information to patients who decide not to be transported by ambulance to the hospital. The information on the form is designed to assist the patient in making an informed decision. A copy of this form, signed by the patient, becomes part of the patient's medical record.
- **D. Authorization Form:** PHI may only be disclosed to another person if the person named in the personal information has previously signed an authorization form to allow that information to be disclosed.
- **E. Medical Records:** The patient care form and the information form shall be considered medical records.
- F. **Employee Medical Records:** Employee medical clearances, drug screens, injury

reports, in-house medical testing, fitness testing records, exposure reports will be considered the employee medical record.

II. District employees will complete annual HIPAA Training as part of the Individual Mandatory Compliance Training Program.

III. Medical information obtained for an employer to carry out its obligations under FMLA, ADA and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees are exempt from the rules of HIPAA. Although these areas are exempt from HIPAA rules, the District requires employees to safeguard the information as they would any other confidential file.

IV. District personnel shall not divulge PHI to any party that has no professional need for that information. This standard includes both written and non-written (verbal) communication.

V. Medical records may be used for quality management purposes as outlined by ORS.

VI. Employee Medical Records:

A. The District's Wellness division is designated as the District's employee medical records keeper and is responsible for the filing and managing of such medical records. District medical records shall be stored electronically and under lock and key. The District's employee medical records keeper and the Wellness Division shall hold the only keys to access these records.

B. The District's medical records shall be stored, per OSHA, for 30 years after retirement.

VII. EMS Incident Records:

A. The District's Administrative Services Division is designated as the District's FireRMS/ePCR Incident medical record keeper and is responsible for managing of such medical records.

B. The medical records keeper may designate other District members to assist with tasks involving medical records, such as delivering documents to District facilities, and assurance issues.

VIII. Patient Care Form:

A. District members complete the patient care form, documenting patients who are assessed, treated or given medical advice.

B. The minimum certification required for a member to be eligible to complete a Patient Care Form is EMT Basic.

C. Policy and instructions for completing the Patient Care Form can be found in the Incident Documentation SOP and the Clackamas Fire District #1 Chart Writing Handbook.

IX. Release of Medical Records:

A. Patients shall have access to their own medical records. The District will provide copies of these records at no charge provided the patient has come to us in person and has photo identification verifying they are the patient. This identification shall be photocopied and a copy of it along with a dated explanation of what was released shall be attached to the completed public records request form. If the patient is a minor, the parents or legal guardians of the patient shall provide sufficient identification to allow the release of copies of the medical records.

B. Individuals with "Power of Attorney" for a patient shall have access to the patient's medical records. The District shall provide copies of these records at no charge provided the individual with the "Power of Attorney" has come to us in person and has photo identification verifying they are the correct person. This identification shall be photocopied and a copy of it along with a dated explanation of the medical record release and a copy of the "Power of Attorney" document shall be attached to the completed public records request form.

C. Medical records may be mailed if the District receives a document to release medical information signed by the patient and notarized by a notary public verifying it is the patient that signed the release of medical information form. This form shall be attached to the completed public records request form. There may be a charge for mailing medical records.

D. Medical records may be mailed if the district receives a document to release medical information signed by an individual with "Power of Attorney" for the patient and notarized by a notary public verifying it is correct person that signed the release of information form. The release of medical record form and a copy of the "Power of Attorney" shall be attached to the completed public records request form. There may be a charge for mailing medical records.

E. Employees may have access to their own medical records. Medical records may be emailed, mailed, faxed or picked up in person after an authorization to release records is signed, dated and specifies what records to release and to whom. Emailed records will be password protected.

X. Use and Disclosure

A. In order to carry out their duties, PHI may be disclosed to employees of Clackamas Fire District #1 who are not involved in the care of the patient.

B. PHI may be disclosed to clerical staff who are responsible for entering patient data into electronic databases or fulfilling public records requests.

C. PHI may be disclosed to EMTs and paramedics who are conducting quality reviews on medical records prepared by other EMTs or paramedics.

D. PHI may be disclosed for the following public policy purposes:
    1. As required by law,
    2. For public health activities,
    3. To report victims of abuse, neglect, or domestic violence,
    4. For judicial and administrative proceedings,
    5. For law enforcement purposes,
    6. For people who are deceased,
    7. For limited research activities,
    8. To avert a threat to health and safety, and
    9. Certain other specialized government functions.
    10. *Questions about whether PHI may be disclosed should be directed to the Privacy Officer.*

XI. Corrective Action/Enforcement

A. Any employees, volunteers, or interns found to have violated this policy or the HIPAA Policies may be subject to disciplinary action in accordance with applicable District policies and procedures, up to and including termination of employment. Additional civil and/or criminal punishments may be applicable.

XII. Complaint Procedure

A. This policy provides patients with certain fundamental rights with respect to their PHI. They have a right to access their PHI, they have a right to request amendments to their PHI, they have a right to an accounting of disclosures of PHI, and they have a right to the District's privacy notice. If patients believe that any of these rights have been violated, they should be directed to the Privacy Officer.

XIII. Privacy Notice

A. Any patient, or any person who may be a patient, is entitled to a copy of the District's privacy notice. Any District employee may provide a copy of that notice, or the patient may be directed to the administrative offices for that notice. The most current privacy notice will be posted on the District's website and will indicate the revision date in the top left hand corner. The District's privacy notice is attached as Appendix B.

XIV. Administrative, Technical, and Physical Safeguards

A. The District will develop and adopt necessary and appropriate HIPAA Policies, which will include, among other things, the technical, physical, and administrative safeguards required to ensure the confidentiality, integrity, and availability of electronic PHI and protect PHI against reasonably anticipated threats or hazards and unauthorized uses or disclosures. The District designates the EMS Chief as the HIPAA Security Officer. Some of those safeguards include:

1. Personnel should not leave medical records or other documents containing PHI on desks or workspaces such that the PHI may be viewed by others.
2. Physical transport of copies of medical records or other documents containing PHI will be performed in such a way so as to protect the records from being lost, stolen, or otherwise observed.
3. Business associates, including vendors storing records, physicians, hospitals, and others with whom the District has a formal or contractual relationship, must agree to protect PHI at least to the same level as the district. See the District's form business associate contract attached as Exhibit C.
4. Information Technology services staff will ensure that appropriate password protection, firewalls, and backup provisions are in place to protect PHI that is stored electronically.
5. When electronic data entry is implemented, the information services staff will ensure that security is appropriately maintained for electronic transmission of data.
6. In addition to the administrative and technical safeguards provided in this procedure and in compliance with the HIPAA Security Rule, the District will take steps to ensure physical safeguards (physical measures, policies, and procedures) to protect the District's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

CERTIFIED

FIRE CHIEF
FRED CHARLTON

APPENDIX A: DISCLOSURE AUTHORIZATION FORM

I authorize to use and disclose a copy of the specific health information described below regarding _____.
(Print name of individual whose information will be used or disclosed)
The health information to be used and/or disclosed consists of (describe information to be used/disclosed as specifically as you can, use additional pages if necessary):
_____
_____

The health information may be disclosed to (Name and address of recipient or recipients):
_____
_____

for the purpose of (describe each purpose of disclosure or indicate that the disclosure is at the request of the individual, use additional pages if necessary):
_____
_____

If the information to be disclosed contains any of the types of records or information listed below, additional laws relating to the use and disclosure of the information may apply. I understand and agree that this information will only be disclosed if I place my initials in the applicable space next to the type of information.

_____ HIV/AIDS information
_____ Mental health information
_____ Genetic testing information
_____ Drug/alcohol diagnosis, treatment, or referral information.

I understand that the information used or disclosed pursuant to this authorization may be subject to redisclosure and no longer be protected under federal law. However, I also understand that federal or state law may restrict redisclosure of HIV/AIDS information, mental health information, genetic testing information and drug/alcohol diagnosis, treatment or referral information.

You are not required to sign this authorization. Refusal to sign the authorization will not affect your treatment, payment, enrollment or eligibility for benefits. The only circumstance when refusal to sign means you will not receive health care services is if the health care services are solely for the purpose of providing health information to someone else and the authorization is necessary to make that disclosure.

You may revoke this authorization in writing at any time. If you revoke the authorization, the

information described above will no longer be used or disclosed for the purposes described in this authorization. The only exception is when Clackamas Fire District #1 has taken action in reliance on the authorization.

To revoke this authorization, please send a written statement to Clackamas Fire District #1 EMS Chief, 11300 SE Fuller RD, Milwaukie, OR 97222 and state that you are revoking this authorization.

I have read and understand this authorization. Unless earlier revoked, this authorization expires _____. (applicable date or event)

By: _____ Date: _____

(Signature of individual or personal representative)

Description of personal representative's authority if applicable:

_____

I received a copy of this signed authorization _____

PLACE LABEL HERE

AUTHORIZATION TO RELEASE MEDICAL INFORMATION

I authorize the Clackamas Fire Wellness Program to release the following records for the purpose of patient care. This authorization shall begin immediately and remain in effect for one (1) year. I understand that I can revoke this authorization at any time in writing, but that revoking this authorization will not affect disclosures made or actions taken before the revocation is received.

I would like my records RELEASED to: ✔ Myself ☐ Medical provider (please provide contact information below)

The records I want to be RELEASED are (check all that apply):

Pre-Hire and Annual Testing: ✔ Lab Results

Other Testing:

☐ Hearing Test ☐ TB Test Form ☐ Immunization Record

☐ Vision Test ☐ Spirometry Test ☐ REsting EKG

☐ UA Dip ☐ Individual Profile

The records that will be release are for the current year testing. If you would like additional records, please specify year and which records:

I would like to receive my records by the following way: (check all that apply):

☐ Emailed to clackamasfire.com email, with password protection.

☐ Emailed to personal email, with password protection: _____

☐ Paper copy from Wellness ☐ Released to Medical Provider:

Medical provider name:

Fax/Number/Email:

* All Wellness originated ePHI is password protected.

In the event that I need to be contacted to talk about my results (Lab or UA), this is the best phone number to contact me:

Phone number:

☐ It is ok to leave a message regarding my health. ☐ It is NOT ok to leave a message regarding my health.

Signature: _____

Patient Date Time

For Office Use Only:	Date results sent:	☐ Email	☐ Paper Copy	Initials:
Follow Up:	1st notification:	☐ Talked to Patient	☐ Left message	Initials:
	2nd notification:	☐ Talked to Patient	☐ Left message	Initials:

APPENDIX B: PRIVACY NOTICE

REVISION DATE: December 15, 2017

CLACKAMAS COUNTY FIRE DISTRICT #1

NOTICE OF PRIVACY PRACTICES

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

If you have questions about this notice, please contact the District's Privacy Officer at Privacy Officer at (503) 742-2642.

All District employees, volunteers, and interns will follow the policies set out in this notice. These policies apply to all records about your care or treatment that have been created by the District's employees, volunteers, or interns and any business associates of the district. You may receive additional privacy notices from your other healthcare providers.

Our Responsibilities

We are required by law to maintain the privacy of your Protected Health Information (PHI) and provide you a description of our privacy practices. We will abide by the terms of this notice**.**

How We May Use and Disclose Your Protected Health Information (PHI)

Uses and Disclosures That Do Not Require Your Authorization

For Treatment

We may use or disclose your PHI to provide care and treatment to you or in order for others to provide treatment to you. For example, we may disclose your PHI to physicians, nurses and other health care personnel involved in your care and treatment.

For Payment

We may use and disclose PHI about your care to bill and collect payment from you, your insurance company, or a third party for the treatment provided. For example, we may use your

PHI to create the bills that we submit to the insurance company, or we may disclose medical information to our business associates who perform billing and claims processing or other services for us. We may also disclose your PHI to another health care provider or insurance company for their payment-related activities.

For Health Care Operations

Fire District personnel and/or members of our quality improvement committee may use information on your health record to evaluate the quality of care and treatment in your case. The results of this evaluation will be used to continually improve the quality of care for all patients we serve. We may also provide your PHI to our attorneys, accountants or other consultants to ensure that we are complying with applicable laws.

Special Situations

We may use or disclose health information about you without your permission for the following purposes, subject to all applicable legal requirements and limitations:

- To Avert a Serious Threat to Health or Safety. We may use and disclose health information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.
- Required by Law. We will disclose health information about you when required to do so by federal, state or local law.
- Research. We may use and disclose health information about you for research projects that are subject to a special approval process. We will ask you for your permission if the research will have access to your name, address or other information that reveals who you are, or will be involved in your care at the office.
- Organ and Tissue Donation. 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 such donation and transplantation.
- Military, Veterans, National Security and Intelligence. If you are or were a member of the armed forces, or part of the national security or intelligence communities, we may be required by military command or other government authorities to release health information about you. We may also release information about foreign military personnel to the appropriate foreign military authority.
- Workers' Compensation. We may release health information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

· Public Health Risks. We may disclose Health Information for public health activities. These activities generally include disclosures to prevent or control disease, injury or disability; report births and deaths; report child abuse or neglect; report reactions to medications or problems with products; notify people of recalls of products they may be using; a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

· Health Oversight Activities. We may disclose health information to a health oversight agency for audits, investigations, inspections, or licensing purposes. These disclosures may be necessary for certain state and federal agencies to monitor the health care system, government programs, and compliance with civil rights laws.

· Data Breach Notification Purposes. We may use or disclose your Protected Health Information to provide legally required notices of unauthorized access to or disclosure of your health information.

· Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose Health Information in response to a court or administrative order. We also may disclose Health Information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

· Law Enforcement. We may release Health Information if asked by a law enforcement official if the information is: (1) in response to a court order, subpoena, warrant, summons or similar process; (2) limited information to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime even if, under certain very limited circumstances, we are unable to obtain the person's agreement; (4) about a death we believe may be the result of criminal conduct; (5) about criminal conduct on our premises; and (6) in an emergency to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

· Coroners, Medical Examiners and Funeral Directors. We may release health information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or to determine the cause of death. We also may release Health Information to funeral directors as necessary for their duties.

· Information Not Personally Identifiable. We may use or disclose health

information about you in a way that does not personally identify you or reveal who you are.

· Disaster Relief. We may disclose your Protected Health Information to disaster relief organizations that seek your Protected Health Information to coordinate your care, or notify family and friends of your location or condition in a disaster. We will provide you with an opportunity to agree or object to such a disclosure whenever we practically can do so.

· Family and Friends. We may disclose health information about you to your family members or friends 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 or friends if we can infer from the circumstances, based on our professional judgment that you would not object. For example, we may assume you agree to our disclosure of your personal health information to your spouse when you bring your spouse with you into the exam room during treatment or while treatment is discussed.

In situations where you are not capable of giving consent (because you are not present or due to your incapacity or medical emergency), we may, using our professional judgment, determine that a disclosure to your family member or friend is in your best interest. In that situation, we will disclose only health information relevant to the person's involvement in your care. For example, we may inform the person who accompanied you to the emergency room that you suffered a heart attack and provide updates on your progress and prognosis. We may also use our professional judgment and experience to make reasonable inferences that it is in your best interest to allow another person to act on your behalf to pick up, for example, filled prescriptions, medical supplies, or x-rays.

Other Uses and Disclosures of Your Protected Health Information (PHI)

We will not use or disclose your health information for any purpose other than those identified in the previous section without your specific, written Authorization. We must obtain your Authorization separate from any Consent we may have obtained from you. If you give us Authorization to use or disclose health information about you, you may revoke that Authorization, in writing, at any time. If you revoke your Authorization, we will no longer use or disclose information about you for the reasons covered by your written Authorization, but we cannot take back any uses or disclosures already made with your permission.

If we have HIV or substance abuse information about you, we cannot release that information without a special signed, written authorization (different from the Authorization and Consent

mentioned above) from you. In order to disclose these types of records for purposes of treatment, payment or health care operations, we will have to have both your signed Consent and a special written authorization that complies with the law governing HIV or substance abuse records.

Your Health Information Rights

You have the following rights related to your health care records maintained by Clackamas County Fire District #1:

- The Right to Inspect and Copy: Except for very limited circumstances, you have the right to inspect and copy medical information that may be used to make decisions about your care. Requests to inspect must be submitted in writing and addressed to our Privacy Officer. In certain situations we may deny your request. If this occurs, you will be notified in writing of the reason for denial and your rights with regard to having the denial reviewed.

- Right to an Electronic Copy of Electronic Medical Records: If your Protected Health Information is maintained in an electronic format (known as an electronic medical record or an electronic health record), you have the right to request that an electronic copy of your record be given to you or transmitted to another individual or entity. We will make every effort to provide access to your Protected Health Information in the form or format you request, if it is readily producible in such form or format. If the Protected Health Information is not readily producible in the form or format you request your record will be provided in either our standard electronic format or if you do not want this form or format, a readable hard copy form. We may charge you a reasonable, cost-based fee for the labor associated with transmitting the electronic medical record.

- The Right to Amend: If you believe that the PHI we have about you is incomplete or incorrect, you may ask us to amend it. You have a right to request an amendment so long as the information is kept by the District. Any request must be submitted in writing and must provide support for the amendment. We may deny your request for an amendment if it is not in writing and does not provide a reason for the amendment. We may deny your request for other reasons. If your request is denied, you will be notified in writing of the reason for denial, and a note will be made to your record stating that you requested an amendment.

- The Right to an Accounting of Disclosures: You have a right to request an accounting of disclosures of your PHI. This is a list of instances in which we have disclosed your PHI for

purposes other than: treatment, payment, healthcare operations, disclosures permitted by our privacy practices or law, for disaster relief or national security purposes, or disclosures to law enforcement. Requests for a list of disclosures must be submitted in writing to our Department Privacy Officer.

- The Right to Request Restrictions: You have the right to request a restriction or limitation on the PHI we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose to family members or friends involved in your care, or payment of care. Any such request must be submitted in writing to our Departments Privacy Officer. We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

- Right to Get Notice of a Breach: You have the right to be notified upon a breach of any of your unsecured Protected Health Information.

- The Right to Request Confidential Communications: You have the right to request that we send information to you at a specific address (for example, work rather that home) or in a specific manner (for example, by e-mail rather than regular mail). We will agree to your request as long as it is not disruptive to our operations. You must make any such request in writing, addressed to our Privacy Officer.

- The Right to a Paper Copy of this Notice: You have the right to request a paper copy of this notice at any time. You may obtain a copy of this Notice by contacting our Privacy Officer at (503) 742-2600.

To exercise any of your rights, please obtain the required forms from our Privacy Officer and submit your request in writing.

CHANGES TO THIS NOTICE

We reserve the right to change our privacy practices and to make such changes applicable to the health information we obtained about you before the change, as well as to information we may receive in the future. You may obtain a copy of any revised Notice by contacting our Privacy Officer at (503) 742-2600. We will also make any revised Notice available at the district's website located at **www.clackamasfire.com**

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint by calling our

Privacy Officer at 503-742-2600. Complaints may also be filed with the Secretary of the Department of Health and Human Services. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Bill Conway, Division Chief - EMS
Clackamas Fire District #1 Privacy Officer

BUSINESS ASSOCIATE AGREEMENT

BETWEEN: _____, **(Covered Entity)**

AND: _____, **(Business Associate)**

DATE: , 20__

RECITALS

WHEREAS, the parties have entered into a business relationship whereby Business Associate provides services to Covered Entity and Business Associate receives, has access to, or creates protected health information in order to provide those services; and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of protected health information disclosed to Business Associate in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and applicable federal regulations, including but not limited to the Standards for Privacy of Individually Identifiable Health Information, 45 Code of Federal Regulations Parts 160 and 164 (collectively known as the Privacy and Security Regulations); and

WHEREAS, the Privacy and Security Regulations require Covered Entity and Business Associate to enter into an agreement containing specific requirements as set forth in, but not limited to, the Privacy and Security Regulations;

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

AGREEMENT

ARTICLE I
DEFINITIONS

1.1 "Breach" means the unauthorized access, acquisition, use, or disclosure of PHI which compromises the security or privacy of that information.

1.2 "Disclose" and "Disclosure" mean, with respect to PHI, the release, transfer, provision of access to, or divulging in any other manner of PHI outside Business Associate's internal operations or to other than its employees.

1.3 "Electronic Protected Health Information" or "e-PHI" means PHI that is transmitted by electronic media (as defined by the Privacy and Security Regulations) or is maintained in electronic media.

1.4 "Protected Health Information" or "PHI" means information that (a) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; (b) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual); and (c) is received by Business Associate from or on behalf of Covered Entity, or is created by Business Associate, or is made accessible to Business Associate by Covered Entity. PHI includes, without limitation, electronic PHI.

1.5 "Secretary" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

1.6 "Services" means the services provided by Business Associate pursuant to the Underlying Agreement(s), or if no such agreement(s) are in effect, the activities, functions, or services that Business Associate performs for or on behalf of Covered Entity.

1.7 "Underlying Agreement" means the agreement for provision of services executed by the Covered Entity and Business Associate, if any.

1.8 "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or

indecipherable to unauthorized individuals through use of a technology or methodology specified in guidance by the Secretary.

1.9 "Use" or "Uses" mean, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such PHI within Business Associate's internal operations.

ARTICLE II
OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 Assurances by Business Associate Regarding PHI. Business Associate warrants that it will comply with the applicable portions of the Privacy and Security Regulations as those regulations apply to business associates. More specifically, and insofar as Business Associate has access to, has been provided with, or will be creating PHI for or on behalf of Covered Entity, Business Associate warrants and agrees as follows:

2.2 Permitted Uses and Disclosures of Health Information. Business Associate will Use and Disclose PHI only in the amount minimally necessary to perform Services for or on behalf of Covered Entity; provided that such Use or Disclosure would not violate the Privacy and Security Regulations if made by Covered Entity. Business Associate is authorized to Use and Disclose PHI under the following conditions and for no other purpose:

2.2.1 As necessary to perform Services for, or on behalf of Covered Entity;

2.2.2 To provide data aggregation services related to the health care operations of Covered Entity (in accordance with the requirements of the Privacy and Security Regulations);

2.2.3 As otherwise directed by Covered Entity, provided that Covered Entity shall not request Business Associate to Use or Disclose PHI in a manner that would not be permissible if done by Covered Entity.

2.2.4 Except as otherwise limited by this Agreement, Business Associate may Disclose PHI for the proper management and administration of Business Associate, provided that with respect to any such Disclosure either:
(a) the Disclosure is required by law (within the meaning of the Privacy and Security Regulations); or
(b) the Disclosure would not otherwise violate Oregon or federal law and Business Associate obtains reasonable written assurances from the person to whom the information is to be

Disclosed that such person will hold the information in confidence and will not Use or further Disclose such information except as required by law or for the purpose(s) for which it was Disclosed by Business Associate to such person, and that such person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.3 Patient's Rights Under the HITECH Act. Business Associate understands and agrees to cooperate with Covered Entity to comply with applicable requirements of the HITECH Act.

2.4 Adequate Safeguards for Health Information. Business Associate warrants and agrees that it will implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI in any manner other than as permitted by this Agreement.

2.4.1 Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity.

2.4.2 Business Associate will ensure that any agent, including a subcontractor, to whom it provides PHI that was created, received, maintained, or transmitted on behalf of Covered Entity, agrees to implement reasonable and appropriate safeguards to protect the confidentiality, security, and integrity of the PHI.

2.4.3 Business Associate agrees to alert Covered Entity of any security incident (as defined by the Privacy and Security Rule) of which it becomes aware as well as the steps it has taken to mitigate any potential security compromise that may have occurred. Business Associate further agrees to provide a report to Covered Entity of any loss of data or compromise of information as a result of the incident.

2.5 Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement. Business Associate will cooperate with Covered Entity in the notification of individuals as required by and in the manner set forth in the HITECH Act.

2.6 Availability of Internal Practices, Books and Records. Business Associate agrees to make its internal practices, books, and records relating to the Use and Disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity

available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations. Business Associate will immediately notify Covered Entity of any requests for information made by the Secretary and will provide Covered Entity with copies of any documents produced in response to such request.

2.7 Access to PHI. Business Associate will make PHI maintained by Business Associate in a designated record set available to Covered Entity, or as directed by Covered Entity, to the individual identified as being entitled to access and copy that PHI, within the time frame and in the manner specified by the Covered Entity.

2.8 Amendment of PHI. Business Associate will make PHI maintained by Business Associate in a designated record set available to Covered Entity for the purpose of amendment and will incorporate such amendments into PHI maintained by Business Associate within the time and in the manner specified by Covered Entity.

2.9 Accounting of Disclosures. Upon Covered Entity's request, Business Associate shall provide to Covered Entity an accounting of each Disclosure of PHI made by Business Associate or its employees, agents, representatives or subcontractors.

2.9.1 Business Associate will implement a process to account for any Disclosure of PHI which Covered Entity is required to maintain. Business Associate shall include in the accounting: (a) the date of the Disclosure; (b) the name, and address if known, of the entity or individual who received the PHI; (c) a brief description of the PHI disclosed; and (d) a brief statement of the purpose of the Disclosure. For each Disclosure that requires an accounting under this section, Business Associate will document the information specified in (a) through (d) above, and will securely retain this documentation for six (6) years from the date of the Disclosure.

2.9.2 To the extent that Business Associate maintains PHI in an electronic health record, Business Associate will maintain an accounting of Disclosures made for Treatment, Payment, and Health Care Operations purposes, as those terms are defined by the Privacy and Security Rules, for three (3) years from the date of Disclosure. This requirement shall become effective upon either of the following: (a) on or after January 1, 2014, if Business Associate acquired electronic health record before January 1, 2009; or (b) on or after January 1, 2011, if Business Associate acquired an electronic health record after January 1, 2009, or such later date as determined by the Secretary.

2.10 Use of Subcontractors and Agents. Business Associate shall require each of its agents and subcontractors that receive PHI from Business Associate to execute a written agreement

obligating the agent or subcontractor to comply with all the terms of this Agreement with respect to such PHI.

2.11 Reporting Unauthorized Disclosures of PHI.

2.11.1 Business Associate will report to Covered Entity any and all of the following unauthorized disclosures:

2.11.1.1 Each access, acquisition, Use, or Disclosure that is made by Business Associate, its employees, representatives, agents, or subcontractors but is not specifically permitted by this Agreement;

2.11.1.2 Any security incident of which Business Associate becomes aware. A security incident means the attempted, or successful unauthorized access, acquisition, Use, Disclosure, modification, or destruction of information, or interference with the system operation of an information system; or

2.11.1.3 A Breach of Unsecured PHI.

2.11.2 Business Associate's Notice to Covered Entity

2.11.2.1 Business Associate shall notify Covered Entity's Fire Chief in person or by telephone within 48 hours of the time Business Associate learns of an unauthorized disclosure.

2.11.2.2 Business Associate shall provide a full written report to Covered Entity's Privacy Official within five (5) days of oral notice. Business Associate shall include the following in the written report:

2.11.2.2.1 Detailed information about the unauthorized disclosure and immediate remedial action taken to stop the unauthorized disclosure; and

2.11.2.2.2 Names and contact information of individuals whose PHI has been, or is reasonably believed to have been subject to the unauthorized disclosure.

2.12 Remedies in Event of an Unauthorized Disclosure of PHI. In the event of an unauthorized disclosure of PHI, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of this Agreement.

2.13 Notification Costs Related to Unauthorized Disclosure of PHI. In the event of an unauthorized disclosure of PHI caused by Business Associate or its employees, representatives, agents, or subcontractors, the costs related to notifying the effected individuals shall be borne by Business Associate. Such costs, if appropriate and reasonable under the circumstances, may include the actual cost of notification, setting-up and managing a toll-free number, and credit monitoring.

2.14 Implementation of Red Flags Identity Theft Protection Program. To the extent that the services provided by Business Associate for or on behalf of Covered Entity include regularly extending, renewing, or continuing credit to individuals, or regularly allowing individuals to defer payment for services, including setting up payment plans in connection with one or more covered accounts, as that term is defined in the Federal Trade Commission's Red Flags Rules, Business Associate warrants it will comply with the Red Flags Rules and, specifically, will put in place and implement a written identity theft prevention program designed to identify, detect, mitigate, and respond to suspicious activities that could indicate that identity theft has occurred.

2.15 Security. All PHI sent from Business Associate to Covered Entity in an electronic format will be sent using a method for securing electronic data approved by the Secretary.

2.16 Pattern or Practice by Covered Entity that Violates Agreement. If Business Associate knows of an activity or practice of Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Agreement, Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, Business Associate must terminate the Services if feasible, or if termination is not feasible, report the activity to the Secretary. Within five (5) days of discovery, Business Associate shall provide written notice to Covered Entity of any pattern of activity or practice of Covered Entity that Business Associate believes constitutes a material breach or violation of Covered Entity's obligations under this Agreement, and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure or end the violation.

ARTICLE III
OBLIGATIONS OF COVERED ENTITY

3.1 Privacy Notice. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices to the extent such limitation(s) may affect Business Associate's Use or Disclosure of PHI.

3.2 Security. All PHI sent from Covered Entity to Business Associate in an electronic format will be sent using a method for securing electronic data approved by the Secretary.

3.3 Notification of Breach. Covered Entity agrees to notify required parties in the event there is a Breach of PHI.

3.4 Pattern or Practice by Business Associate that Violates Agreement. If Covered Entity knows of an activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under this Agreement, Covered Entity must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, Covered Entity must terminate the Business Associate's Services if feasible, or if termination is not feasible, report the activity to the Secretary. Within five (5) days of discovery, Covered Entity shall provide written notice to Business Associate of any pattern of activity or practice of Business Association that Covered Entity believes constitutes a material breach or violation of Business Associate's obligations under this Agreement, and shall meet with Business Associate to discuss and attempt to resolve the problem as one of the reasonable steps to cure or end the violation.

ARTICLE IV
TERM AND TERMINATION

4.1 Term and Termination for Cause. The term of his Agreement shall be the same as the term of the Underlying Agreement. In addition to and notwithstanding the termination provisions set forth in the Underlying Agreement, both this Agreement and the Underlying Agreement may be terminated by Covered Entity immediately and without penalty upon written notice by Covered Entity to Business Associate if Covered Entity determines, in its sole discretion, that Business Associate has violated any material term of this Agreement. The terms and conditions of this Agreement shall survive the termination of the Underlying Agreement.

4.3 Termination for Breach of Section 5.2. Covered Entity or Business Associate may terminate the Underlying Agreement and this Agreement upon thirty (30) days written notice in the event (a) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by Covered Entity pursuant to Section 5.2 or (b) Business Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that the Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA.

4.4 Disposition of PHI upon Termination or Expiration. Upon termination or expiration of this Agreement, Business Associate shall either return or destroy, in Covered Entity's sole discretion and in accordance with any instructions by Covered Entity, all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, in the possession or control of Business Associate and its agents and subcontractors. Business Associate shall retain no copies of such PHI. However, if neither return nor destruction of PHI is feasible, Business Associate may retain PHI provided that Business Associate (a) continues to comply with the provisions of this Agreement for as long as it retains the PHI, and (b) limits further Uses and Disclosures of the PHI to those purposes that make the return or destruction of PHI infeasible.

ARTICLE V
MISCELLANEOUS

5.1 Indemnification. Notwithstanding anything to the contrary in the Underlying Agreement, at Business Associate's expense, Business Associate agrees to indemnify, defend, and hold harmless Covered Entity and Covered Entity's employees, directors, officers, subcontractors, and agents against all damages, losses, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) and all liability to third parties arising from any material breach of this Agreement by Business Associate or its employees, directors, officers, subcontractors, agents, or other members of Business Associate's workforce. Business Associate's indemnification obligations pursuant to this paragraph shall survive the expiration or termination of this Agreement.

5.2 Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be required to incorporate procedures to ensure compliance with new developments. The parties specifically agree to take such action as necessary to implement the standards and requirements of HIPAA and other applicable laws relating to the security or confidentiality of PHI. Upon Covered Entity's request, Business Associate agrees to promptly enter into negotiations with Covered Entity concerning the terms of any amendment to this Agreement required by HIPAA or other applicable laws.

5.3 Relationship to Provisions of Underlying Agreement. In the event that a provision of this Agreement is contrary to a provision of an Underlying Agreement, this Agreement shall control. Otherwise, this Agreement shall be construed under, and in accordance with, the terms of the

Underlying Agreement and shall be considered an amendment of and supplement to the Underlying Agreement.

5.4 Modification of Agreement. No alteration, amendment, or modification of the terms of this Agreement will be valid or effective unless it is in writing and signed by Business Associate and Covered Entity.

5.5 Waiver. A waiver by either party of a breach of any provision of this Agreement will not operate or be construed as a waiver of any other provision of this Agreement or of any subsequent breach of the same provision of this Agreement.

5.6 Agreement Drafted By All Parties. This Agreement is the result of arm's length negotiations between the parties and shall be construed to have been drafted by all parties such that any ambiguities in this Agreement shall not be construed against either party.

5.7 Severability. If any provision of this Agreement is held by any court of competent jurisdiction to be invalid, such invalidity will not affect any other provisions of this Agreement, and this Agreement will be construed as if the invalid provision had never been included in this Agreement.

5.8 Section Headings. Section headings are used solely for convenience and are not to be used in construing or interpreting this Agreement.

5.9 No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement.

5.10 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, and will become effective and binding upon the parties at the time all the signatories to this Agreement have signed a counterpart of this Agreement.

5.11 Notices. Any written notices required or permitted by this Agreement will be given: (1) by personal delivery; (2) by facsimile with confirmation sent by United States first class registered or certified mail, postage prepaid, return receipt requested; (3) by bonded courier or by a nationally recognized overnight delivery service; or (4) by United States first class registered or certified mail, postage prepaid, return receipt requested, in each case, addressed to:

Business Associate:	Covered Entity:
_____	_____
Attn: Privacy Officer	Attn: Privacy Officer
_____	_____
_____	_____

Either may change their notice address at any time by written notice that complies with this Section 5.11. Notices shall be deemed received on the earliest of: (a) personal delivery; (b) upon delivery by electronic facsimile with confirmation from the transmitting machine that the transmission was completed; (c) twenty-four (24) hours following deposit with a bonded courier or overnight delivery service; or (d) seventy-two (72) hours following deposit in the U.S. Mail.

5.12 Applicable Law and Venue. This Agreement will be governed by and construed in accordance with the laws of the State of Oregon (without regard to principles of conflicts of laws). The parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated exclusively Lane County Circuit Court, or if appropriate, in the federal district court for the District of Oregon. THE PARTIES BY EXECUTION OF THIS AGREEMENT, HEREBY CONSENT TO THE IN PERSONAM JURISDICTION OF SAID COURTS.

5.13 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Regulations.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement effective as of the date stated above.

COVERED ENTITY	**BUSINESS ASSOCIATE**
_____	_____

By: _____ By: _____

Printed Name: _____ Printed Name: _____

Title: _____ Title: _____

Dated: _____ Dated: _____