Protected Health Information

Personnel – General Provisions

EWU Policy 401-06

Effective November 17, 2017

Authority: EWU Board of Trustees

Proponent: Vice President of Business and Finance

Summary: This policy prescribes standards and procedures for protecting the confidentiality of medical records created, received, transmitted or maintained by those departments designated as Eastern Washington University Healthcare in accordance with the Health Information Portability and Accountability Act of 1996.

History: This policy revises and supersedes Policy 401-06 dated December 3, 2013. It was adopted by the EWU Board of Trustees on November 17, 2017.

1. GENERAL

Eastern Washington University (EWU) is committed to protecting the privacy and security of medical records covered by the Health Information Portability and Accountability Act of 1996 (HIPAA), federal Privacy and Information Security regulations (45 CFR Parts 160 and 164), the Health Information Technology for Economic and Clinical Health (HITECH Act), and state privacy regulations including but not limited to chapter 70.02 RCW. In the course of providing medical treatment to clients of the Dental Hygiene and Communication Sciences and Disorders clinics, EWU may create, receive, transmit, or maintain protected health information (PHI) subject to HIPAA, its related regulations, and state privacy regulations. EWU shall establish administrative, technical, and physical safeguards to secure the confidentiality of such records.

2. DEFINITIONS

a. Business Associate: Any person or entity, other than a member of the EWU workforce, who performs services for or on behalf of EWU Healthcare involving the use or disclosure of PHI, such as billing, information technology, quality control assessments, document destruction, and legal services. Any provider that creates, receives, maintains, or transmits PHI on behalf of EWU Healthcare is a business associate.

b. Protected Health Information (PHI): Health information that identifies an individual, or with respect to which there is a reasonable basis to believe the information can be used to identify an individual, and that is transmitted or maintained electronically or in any other form or medium. The following are not PHI:

(1) educational records covered by the Family Educational Rights and Privacy Act;

(2) medical records of students used only in connection with treatment of the student; and,

(3) employment records held by EWU in its role as an employer.

c. Subcontractor: A person or entity, other than a member of a business associate's workforce, to whom a business associate delegates a function, activity, or service, that creates, receives, maintains or transmits PHI.

d. EWU Workforce Members: Workforce members include EWU faculty, employees, students, trainees, and volunteers. Additionally, Washington State University students who are part of EWU's Communication Sciences and Disorders program and University of Washington students who are part of part of the RIDE program at EWU are considered to be EWU workforce members for the purposes of this policy.

3. DESIGNATION OF HEATLH CARE COMPONENTS

EWU is required by federal law to designate those entities within the University that are required to comply with HIPAA and its related regulations. EWU is a hybrid entity, meaning it has both healthcare components and non-healthcare components. Healthcare components must comply with HIPAA. Non-healthcare components are not required to comply with HIPAA.

a. EWU Healthcare

EWU healthcare components (hereinafter "EWU Healthcare") include the departments of Dental Hygiene and Communication Sciences and Disorders.

b. Other Covered Components

EWU Healthcare, to a limited extent, uses the services the Division of Business and Finance ("Business and Finance") and the Information Technology Division ("IT"). To the extent Business and Finance and IT perform support functions involving the use or disclosure of PHI for or on behalf of EWU Healthcare, including, but not limited to, billing, information technology, quality control assessments, and document retention, they are deemed to be functioning as healthcare components and must comply with HIPAA. For the purposes of this policy,

Business and Finance and IT are considered to be part of "EWU Healthcare" to the extent they perform the functions listed above.

c. Non-Healthcare Components

All other components of the EWU are considered to be non-healthcare components. A component of EWU Healthcare may not disclose PHI to a non-healthcare component in any situation where such disclosure would be prohibited by HIPAA if the healthcare component and non-healthcare component were separate legal entities.

4. UNIVERSITY PRIVACY & SECURITY COMPLIANCE OFFICERS

a. University HIPPA Privacy Officer

The Communication Sciences and Disorders Clinic Director shall serve as the University HIPPA Privacy Officer (Privacy Officer). The Privacy Officer oversees the EWU HIPAA privacy compliance program and is responsible for the following:

(1) Developing and implementing policies, procedures, internal controls, forms and tools related to federal and state privacy laws and regulations.

(2) Auditing and monitoring system-wide practices to ensure compliance.

(3) Receiving and investigating complaints.

(4) Providing information about matters covered by the Notice of Privacy Practices.

(5) Serving as the contact point for patients who wish to exercise their privacy rights.

(6) Ensuring workforce members are educated about their responsibilities related to federal and state privacy laws and regulations.

(7) Maintaining records in accordance with state and federal requirements.

(8) Monitoring regulatory developments and recommending program modifications as needed.

(9) Serving as liaison with the Attorney General's Office.

b. Security Compliance Officer

The IT Security Manager & Engineer, or designee, shall serve as the EWU Security Compliance Officer (SCO). The SCO will evaluate information systems to ensure compliance with HIPAA security requirements. This includes any systems that are used by EWU Healthcare to create, store, receive or transmit PHI.

5. EMPLOYEE EDUCATION AND TRAINING

EWU Healthcare workforce members must:

(1) Complete and sign a privacy, confidentiality, and data security agreement within 30 days of hire or if their job duties change to include access to PHI; and,

(2) Complete HIPAA Training within 30 days of hire or reassignment to a position including access to PHI.

EWU Healthcare components are responsible for providing training to their workforce members.

6. PRIVACY CONCERNS AND COMPLAINTS

a. Policy

EWU will provide patients with a Notice of Privacy Practices that complies with the requirements of 45 CFR § 164.520. The notice will describe how EWU may use or disclose their PHI, as well as the procedure for patients to restrict some uses or disclosures. EWU is committed to ensuring individual privacy and providing timely responses to complaints regarding EWU privacy practices. EWU will mitigate, to the extent practicable, any harmful effect that is known to EWU of an unlawful use or disclosure of PHI.

The Privacy Officer, or designee, receives and handles privacy complaints[1] from patients and workforce members. Allegations of noncompliance with EWU privacy policies and practices will be promptly and thoroughly investigated by the Privacy Officer or designee. Findings will be documented in writing and reported to the appropriate authorities.

Patients are informed of their right to file such complaints in the Notice of Privacy Practices. The Notice of Privacy Practices is distributed to patients and posted in the locations where EWU provides health care services. The Notice of Privacy Practices is available to the public on EWU's website. Workforce members who handle PHI are informed of their rights to file a complaint and make inquiries about EWU privacy practices during the mandatory privacy training.

Workforce members are required to cooperate with all compliance investigations. Failure to cooperate will not prevent the investigation from proceeding, but may result

[1] Complaints and investigations regarding potential breaches of information security are addressed in EWU Policy 203-01, Information Security.

in a second investigation of the workforce member for non-cooperation.

Workforce members who violate EWU policies will be subject to appropriate corrective actions. Information discovered during the fact-finding process that suggests a potential violation of other University policies may be referred to the appropriate University official.

b. EWU Intake Points for Privacy Inquiries and Complaints

Privacy inquires and complaints may be submitted in writing (U.S. Mail or email) or by telephone to:

Privacy Officer

310 North Riverpoint Blvd.

Box V

Spokane, WA 99202

509-828-1333privacyofficer@ewu.edu

c. Complaint Review and Investigation

Individuals who file a complaint must identify the conduct they believe is in violation of EWU policies. All complaints received directly by EWU Healthcare must be referred to the EWU Privacy Officer for assessment and processing.

Upon receipt, the Privacy Officer will evaluate and acknowledge the complaint in writing within ten (10) business days. The acknowledgement will include a description of the process and expected timeline for completion of the investigation.

When a complaint is about an EWU workforce member, if appropriate, the Privacy Officer will notify human resources about the nature of the complaint. Notification includes a description of the process and expected timeline for completion of the investigation.

EWU coordinates management of complaints with appropriate institutional authorities.

Where applicable, investigations will be carried out per EWU Guideline 401-01, Investigations.

d. Notification of Outcome

The complainant will be notified of the outcome of the investigation if the Privacy Officer is provided with the complainant's name and necessary contact information.

e. Documentation & Retention

All complaints and the outcomes of any related investigations must be documented. Such documentation is retained in accordance with EWU record retention policies and applicable state and federal laws. In general, compliance investigation records are retained for a minimum of six (6) years from the last date of service to the patient or the last date the record was used by EWU, whichever is later. Records related to treatment of minors are maintained for at least ten (10) years, or no less than three (3) years following the patient's eighteenth birthday. When an EWU policy requires retention for a longer period of time than the law requires, record retention will be consistent with the EWU policy.

A copy of EWU's response to any privacy complaint filed by a patient must be maintained in the patient's medical records.

f. Review of Investigative Findings

If a complainant is not satisfied with the results of an investigation, the complainant may request a review by the Vice President of Business and Finance. The Vice President, or designee, after reviewing the complaint and investigative findings, will respond to the complainant in writing. The written response will inform the complainant of their right to file a complaint with the United States Department of Health and Human Services, Office for Civil Rights (OCR) and provide the complainant with OCR's contact information.

g. Making Privacy Complaints to U.S. Department of Health and Human Services

Individuals may submit privacy complaints to OCR. Complaints to OCR should be directed to:

Office for Civil Rights

U.S. Department of Health & Human Services

2201 Sixth Avenue - Mail Stop RX-11

Seattle, WA 98121

(206) 615-2290; (206) 615-2296 (TDD)

(206) 615-2297 FAX

h. Responding to Privacy Practice Complaints Received from OCR

If an EWU workforce member receives a privacy practice complaint from OCR, the workforce member must immediately forward the complaint to the Privacy Officer. The Privacy Officer evaluates the complaint, makes the appropriate notifications as noted above, coordinates handling of the complaint, serves as primary point of contact for all communications with the OCR, and maintains all required documentation.

i. Non-Retaliation

EWU will not intimidate, threaten, coerce, or retaliate against persons for filing good faith complaints with the University, OCR, or other governmental agencies or for testifying, assisting or participating in investigations, compliance reviews, proceedings or hearings, or for opposing real or perceived unlawful acts or practices

provided the opposition is reasonable and does not involve a disclosure of PHI that would be prohibited under the law.

7. BUSINESS ASSOCIATES

a. Business Associate Agreement Required

EWU Healthcare is required to enter into agreements governing the confidentiality of PHI with any Business Associates. Before any disclosure of PHI is made to a Business Associate, the Business Associate must agree to the terms of EWU's business associate agreement. Business Associates are independently required to comply with HIPAA's privacy and security rules. Prior to entering into a contract, EWU is required to obtain satisfactory assurance that Business Associates will appropriately safeguard PHI that may be created or received on its behalf. A Business Associate may disclose PHI to a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on the Business Associate's behalf, only if the Business Associate obtains satisfactory assurance that the subcontractor will appropriately safeguard the information and agree to the same restrictions and conditions that apply to the Business Associate.

The purpose of this section is to specify the procedure for determining which entities are business associates and entering into contracts with such entities.

b. Procedure

Department managers or other individuals contracting with another party must determine whether the other party is a Business Associate. A person or entity is a Business Associate when all three of the following criteria are met:

(1) The outside entity or individual is not a member the EWU Healthcare workforce;

(2) The outside entity or individual will be or is performing a service or activity "for" or "on behalf of" EWU Healthcare; and

(3) The services or activities of the outside entity or individual include creating, receiving, maintaining or transmitting PHI. (Note: If an entity maintains PHI on behalf of EWU, it is a business associate even if the entity does not actually view the PHI.)

If the other party to a contract is a Business Associate, the department manager or other person entering into the contract on behalf of EWU must work with Business & Auxiliary Services to complete the Business Associate Agreement. Business & Auxiliary Services will attach the Business Associate Agreement to the contract. Business & Auxiliary Services will make an inventory of all business associate agreements.

If the contract or purchase order is with another government agency, a memorandum of understanding, rather than a business associate agreement, is required. The department manager or other person entering into the contract on behalf of EWU will work with Business & Auxiliary Services to complete a business associate memorandum of understanding. Business & Auxiliary Services will attach a copy of the business associate memorandum of understanding will be attached to the memorandum and make a record of such agreement in the Business Associate Inventory.

c. Data Sharing Agreement Required

EWU Policy 203-01 prescribes university standards for data security. Additionally, a data sharing (security) agreement is required when confidential university data is provided to EWU business partners, vendors, or other outside parties. A Data Security Agreement shall be used when one or more of the following scenarios occur:

(1) EWU transfers confidential data to a contractor's offsite location.

(2) A Contractor accesses EWU systems containing confidential data.

(3) A Contractor provides hardware or software support for EWU systems and may have incidental access to confidential data.

(4) A Contractor provides a hardware and/or software system that is preconfigured to store or process confidential data in a manner that provides the contractor with incidental access to confidential data.

If any of the above scenarios occur, a Data Security Agreement must be included in addition to the Business Associate Agreement as an addendum to the contract for the purchase of goods or services.

d. Violations of the Business Associate Agreement

(1) Suspected or Known Violations: If a member of the EWU workforce suspects or discovers that a Business Associate has violated a business associate agreement, the person should immediately report the violation to the Privacy Officer.

(2) Substantiated Violations: If the Privacy Officer determines that a Business Associate has failed to comply with the requirements of a business associate agreement, the Privacy Officer will work with legal counsel to determine what remedies are available to EWU and whether the contract may be terminated. When EWU knows of a pattern of activity or practice that constitutes a material breach or a violation of the Business Associate's obligations under the agreement,

EWU must take reasonable steps to remedy the breach or end the violation. Reasonable steps may include termination of the agreement.

8. BREACHES

a. Definitions

(1) Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA privacy rules that compromises the security or privacy of the PHI.

An improper use or disclosure of PHI is presumed to be a breach unless the Privacy Officer performs a risk assessment and determines that there is a low probability the PHI has been compromised. In conducting the risk assessment, the Privacy Officer should consider:

(a) The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification;

(b) The identity of the unauthorized person who used the PHI or to whom it was disclosed;

(c) Whether the PHI was actually acquired or viewed; and,

(d) The extent to which risk to the PHI has been mitigated.

The following disclosures are not breaches:

(a) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a EWU Healthcare or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA privacy rules.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at EWU Healthcare or Business Associate to another person authorized to access PHI at the same EWU Healthcare or Business Associate, or organized health care arrangement in which EWU Healthcare participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA privacy rules.

(c) A disclosure of PHI where EWU Healthcare or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Unsecured PHI means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the following methods:

(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule; or,

(b) The media on which the PHI is stored or recorded has been destroyed.

b. Discovery

A breach shall be treated as discovered by EWU Healthcare on the first day an EWU workforce member knows of the breach or, in exercising reasonable diligence, should have known of the breach. All EWU workforce members are required to notify the Privacy Officer immediately of any known or suspected breach.

A workforce member is permitted to disclose PHI to either a health oversight agency or a university retained attorney, if they become aware of unethical or inappropriate behavior committed by another workforce member.

c. Notification to Individuals

Following the discovery of a breach of unsecured PHI, EWU shall notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

(1) Timing of Notification: Except for a law enforcement delay, EWU shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(2) Content of Notification: Notification to the individual shall be written in plain language and include, to the extent possible:

(a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(b) A description of the types of unsecured PHI that were involved in the breach;

(c) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what EWU is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(e) Contact information for the Privacy Officer if the individual has questions or needs additional information.

(3) Method of Notification: Notification to the individual shall be provided in the following form:

(a) Written notice. Notice of the breach shall be sent by first class mail to the affected individual at the last known mailing address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. If EWU knows the individual is deceased and has the address of the next of kin or personal representative of the individual, the notification shall be sent by first class mail to either the next of kin or personal representative of the individual.

(b) Substitute notice. If EWU does not have current, adequate contact information for an individual, notice shall be communicated by a method reasonably calculated to reach the individual in accordance with 45 C.F.R. § 164.404.

d. Notification to the Media

If the breach involved unsecured PHI of more than 500 residents of a state, EWU shall notify prominent media outlets serving such state of the breach no later than 60 calendar days after the breach is discovered, unless a delay is needed for law enforcement purposes.

e. Notification to the Secretary

EWU will notify the Secretary of the Department of Health and Human Services (HHS) of any breaches of unsecured PHI. If the breach involves the unsecured PHI of less than 500 individuals, the Privacy Officer will maintain a log of all such breaches and submit the log to HHS at the end of the calendar year. If the breach involves the unsecured PHI of 500 or more individuals, EWU will notify HHS of the breach at the same time it provides notification to the affected individuals.

EWU will also determine whether it is necessary to notify the Washington State Attorney General's Office of the breach pursuant to RCW 42.56.590.

f. Business Associate's Obligation to Notify EWU of a Breach

A Business Associate shall, following the discovery of a breach of unsecured PHI, notify EWU within five (5) working days of the breach or suspected breach, provide all necessary information, and fully cooperate with any investigations regarding the breach.

A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of the business associate.

g. Law Enforcement Delay

If a law enforcement official notifies EWU that the notification required under this policy and HIPAA regulations would impede a criminal investigation or cause damage to national security, EWU shall document the request and delay any necessary notifications in accordance with 45 C.F.R. § 164.412.