**PROCEDURE FOR RECEIVING AND RESOLVING PRIVACY COMPLAINTS**

1. Designation of the EMU Privacy Director as Point of Contact. The Privacy Director shall be responsible for receiving complaints. The Privacy Director's responsibilities include receiving complaints alleging a violation of the HIPAA Privacy and Security Rules, for investigating and resolving such allegations and resolving complaints, and providing information to persons who request additional information about matters addressed in the *Notice of Privacy Practices* ("NPP"). The EMU Privacy Director, in consultation with Legal Affairs, is responsible for determining whether a confirmed violation of the Privacy and/or Security Rules constitutes a Breach of unsecured PHI under the HITECH Act, tracking such determinations, and providing notification of Breaches to individuals, regulatory agencies, and the media, as appropriate. Privacy Director may delegate some or all of the responsibility for intake, communication, and investigation at its discretion.

2. Inform Persons of Their Right To Complain. The Notice of Privacy Practices shall inform persons that they may complain to EMU's Privacy Director and/or to the Secretary if they believe their privacy rights have been violated. The NPP shall identify the EMU Privacy Director for receiving complaints and give a brief description of how the person may file a complaint. The NPP shall also contain a statement that the person will not be retaliated against for filing a complaint.

3. Filing a Complaint. EMU shall provide the following assistance when a person wishes to file a complaint:

    1. **Verbal or Written Complaints to EMU**. If any person or organization wishes to complain to EMU, the person shall contact or shall be directed to EMU Privacy Director or designee. The Officer, or its designee, shall ask the person whether he or she wishes to submit a written or oral complaint.

    a) Written complaints. If the person wishes to submit a written complaint, the person may be directed to a form that captures the nature of the complaint, relevant dates, individuals involved and any other information necessary to enable a review of the complaint.

    b) Verbal complaints. If the person wishes to submit a verbal complaint, the Privacy Director, or its designee, shall ask the person to explain the complaint in sufficient terms to enable the Officer to investigate, review, and resolve the complaint. The Officer, or its designee, shall document the verbal complaint in writing.

Complaints to HHS. If a person wishes to complain to the Secretary, the person shall be referred to the NPP, which contains the information sufficient to make a written complaint, either in paper or electronic form.

Determination of Privacy Rule Violation. All complaints alleging a violation of the HIPAA Privacy and/or Security Rules must be reported to EMU's Privacy Director. Not every violation of the Privacy Rule constitutes a Breach of unsecured PHI. To determine whether a Breach has occurred, the Privacy Director is responsible for conducting a fact-specific analysis in accordance with the requirements of the HITECH Act, and maintaining documentation of such determinations for a period of six years. Once a Breach of unsecured PHI is determined, the Privacy Director is responsible for notifying each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed. The Privacy Director shall maintain a record documenting privacy complaints received and their disposition, if any. In addition documentation of risk assessments or application of any exceptions to the definition of "Breach" to demonstrate that notification was not required. Documentation must be maintained in written or electronic form for 6 years from the date of the complaint.

Upon determination that one or more members of the workforce has failed to comply with the privacy policies and procedures and/or the Privacy Standards, the Privacy Director shall refer the workforce member(s) to Human Resources for sanctions/discipline in accordance with EMU Policy on Discipline for Violations of Privacy or Security of Protected Health Information (PHI) or Other Sensitive Information. All workforce members are subject to disciplinary action up to and including termination for failure to adhere to this EMU policy.

Providing Notice of Breach.

1. The details of such notice shall be in accordance with the requirements of HIPAA, the HITECH Act, and any subsequent amendments thereto.

2. Such notice must occur without unreasonable delay and in no case later than 60 calendar days after the date the Breach was discovered by EMU workforce.

3. Method of Notice to Individuals:

Notice to the Individual. Written notice to the individual (or if applicable, the individual's parent or personal representative) or next of kin if the individual is deceased, at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual);

Insufficient or Out-of Date Contact Information. In the case where there is insufficient or out-of-date contact information, or if some notices have been returned as undeliverable, substitute notice must be provided as soon as reasonably possible after EMU becomes aware that it has insufficient or out-of-date contact information for one or more affected individuals. However, in the case of decedents, substitute notice is not required for the next of kin or personal representative in cases where EMU either does not have contact information or has out-of-date contact information for the next of kin or personal representative.

i. In the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period of 90 days as specified by the Secretary of Health & Human Services) on the web site of the University (use of a prominent hyperlink from the home page is permissible) or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside. This substitute notice must include a toll-free telephone number, active for 90 days, that individuals can call to find out whether their unsecured PHI may be included in the Breach;

ii. In the case of fewer than 10 individuals for whom EMU has insufficient or out-of-date contact information to provide written notice, EMU may provide substitute notice through an alternative form of written notice, by telephone or other means (e.g., email, even if the patient has not agreed to electronic notice.)

Additional Notice in Urgent Situations: In cases that EMU deems are urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.

Notice of Breach to Media. If a Breach of unsecured PHI involves more than 500 residents of any one State or jurisdiction, the Privacy Director will work with Legal Affairs to provide notice to prominent media outlets as required under the HITECH Act. Such notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

Notice of Breach to the Secretary of Health & Human Services. The Secretary must be notified of Breaches of unsecured PHI in accordance with the following:

a. For Breaches involving 500 or more individuals, the Privacy Director is responsible for providing notice to the Secretary immediately (without unreasonable delay and in no case later than 60 calendar days following discovery of the Breach) in a manner specified on the HHS website.

b. For Breaches involving less than 500 individuals (regardless of whether the Breach involved more than 500 residents of a particular state or jurisdiction), notice must be provided by the EMU Privacy Director to the Secretary in accordance with procedure, and in all cases, no later than 60 days after the end of each calendar year in which such Breaches were determined.

Notification of a Breach committed by a Business Associate

Section 13402(b) of HITECH requires a business associate ("BA") to notify the Covered Entity (EMU) when it discovers a Breach of unsecured PHI involving the Covered Entity's patients. In such cases, EMU is required to notify the individuals involved in such Breach in the same manner set forth above.

No Intimidating or Retaliatory Acts/Waiver of Rights. No member of the workforce will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for the exercise by that individual of any right under the Privacy Standards, or for participation by the individual in any process established by the Privacy Standards. This prohibition applies to any individual filing a complaint with the Secretary; testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the Privacy Standards; or opposing any act or practice of EMU, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the Privacy Standards. No person will be asked to waive his or her rights, including the right to file a complaint with the Secretary, as a condition of treatment or payment.

**VII. REFERENCES**

45 C.F.R. §§ 160.306, 164.520(b)(vi), 164.530(a), (b), (d), (g), (h) (2001)
42 C.F.R. § 482.13(a)(2) (2001) (Medicare Conditions of Participation)

65 Fed. Reg. 82462, 82487, 82550, 82562, 82563, 82600-01, 82746-47, 82748, 82768, 82783, 82801-02, 82821, 82826-28 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

74 Federal Register 42740 - August 2009 (Breach Notification Interim Final Regulation)

78 Federal Register 5566 - January 2013 (Final Rule-Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules)

45 Code of Federal Regulations (CFR) Parts 160 and 164

**Author:**

**Approved by:**