HIPAA Notification in the Event of a Breach of Unsecured Protected Health Information (PHI)

Interim

REG12.60.09 Current Version

Authority: Chancellor

History: Effective: September 19, 2013; Revised: February 2, 2010; October 12, 2010; September 18, 2013; Transitioned from Interim to Permanent: July 17, 2014. Current Interim version revised and approved February 4, 2015.

Related Policies: ECU HIPAA Training

Privacy Complaint Process

Sanctions

Additional Resources: 45 CFR 164 Subpart D: Notification in the Case of Breach of Unsecured Protected Health Information

Department of Health & Human Services: Breach of Unsecured Personal Health Information

ECU Healthcare Components

Guidelines for Media Sanitization

Contact Information: ECU HIPAA Privacy Office, 252-744-5200

Archived Versions:
Version 1
Compare Versions

---

1. Purpose

1.1. East Carolina University's Health Care Components ("ECU's Health Care Components") have a legal duty to provide certain types of notification in the event of a breach of unsecured protected health information ("PHI"). The purpose of this Regulation is to define how ECU's Health Care Components will implement this notification requirement.

2. Definitions

2.1. Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Federal HIPAA privacy rules which compromises the security or privacy of PHI.

2.1.1. A breach does not include:

2.1.1.1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of an ECU Health Care Component if such acquisition, access or use was made in good faith and within the scope of authority of any such individual and does not result in any further improper use or disclosure of PHI.

2.1.1.2. Any inadvertent disclosure of PHI by an individual who is authorized to access PHI at any ECU Health Care Component to another individual authorized to access PHI at the same ECU Health Care Component, business associate or Vidant Medical Center (as part of our organized health care arrangement), provided that the PHI received as a result of such disclosure does not result in any further improper use or disclosure of PHI.

2.1.1.3. A disclosure of PHI where an ECU Health Care Component has a good faith belief that an unauthorized individual to whom such disclosure was made would not reasonably have been able to retain such information.

2.2. Compromises the Security or Privacy of PHI: A breach is

presumed unless the ECU Health Care Component can demonstrate that there is a low probability that the PHI bas been compromised, based on assessment of a group of risk factors.

2.2.1. Risk factors:

2.2.1.1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2.2.1.2. Whether the PHI disclosed violates the minimum necessary standard;

2.2.1.3. The unauthorized person who used the PHI or to whom the disclosure was made;

2.2.1.4. Whether the PHI was actually acquired or viewed; and

2.2.1.5. The extent to which the risk to PHI has been mitigated by the ECU Health Care Component.

2.3. Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through one or more of the following:

2.3.1. Electronic PHI has been encrypted as specified in the HIPAA Security Rules (45 C.F.R. Section 164.304); or

2.3.2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

2.3.2.1. Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. [Redaction is excluded as a means of data destruction.]

2.3.2.2. Electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-00, Guidelines for Media Sanitization, such that PHI cannot be retrieved.

3. Procedure

3.1. Notification to ECU HIPAA Privacy Office

3.1.1. A workforce member or agent of an ECU Health Care Component who suspects that a potential breach has occurred shall immediately notify the ECU HIPAA Privacy Office by calling: 252-744-5200 or 1-866-515-4587; or by email at: healthcareprivacy@ecu.edu.

3.2. Notification to Individuals

3.2.1. Time Period for Notification

The ECU HIPAA Privacy Office shall notify an individual without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a breach of such an individual's unsecured PHI by the ECU Health Care Component.

3.2.2. Breaches Treated as Discovered

A Breach shall be treated as discovered by an ECU Health Care Component as of the first day on which such breach is known or, by exercising reasonable diligence, should have been known to any person.

3.2.3. Content of Notification

Notification as required under this section shall be written in plain language and include, to the extent possible:

3.2.3.1. A brief description of the event, including the date of the breach and the date of discovery of the breach, if known; provided, however, that such description shall not include any information related to any personnel actions taken as a result of such breach;

3.2.3.2. A description of the types of unsecured PHI that were involved in the breach (e.g., name, social security number, date of birth, home address, account number, diagnosis, etc.);

3.2.3.3. Any steps an affected individual should take to protect themselves from potential harm resulting from the breach;

3.2.3.4. A brief description of actions the relevant Health Care Component is taking or has taken to investigate the breach, mitigate harm to affected individuals and to protect against any potential further breaches of unsecured PHI; and

3.2.3.5. Contact procedures for affected individuals to obtain additional information which shall include a toll-free telephone number, email address, website or postal address.

3.2.4. Methods of Individual Notification

3.2.4.1. Written Notice: Notification as required by this Section shall be in writing and sent via first-class mail to the last known address of the affected individual or, if such individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. If the Health Care Component has knowledge that the affected individual is deceased, the Health Care Component may provide such written notification to the next of kin or personal representative of the deceased. Notification required by this section may be provided in one or more mailings as information is available.

3.2.4.2. Substitute Notice: In the event written notification to the affected individual is not possible as a result of insufficient or out-of-date contact information, a substitute form of notice reasonably calculated to reach such individual shall be provided by Health Care Component.

3.2.4.2.1. Substitute notice is not required in the event of insufficient or out-of-date contact information of the next of kin or personal representative of a deceased individual.

3.2.4.2.2. In the event there is insufficient or out-of-date contact information for fewer than ten (10) affected individuals by a breach, substitute notice may be provided by an alternative form of written notice, telephone or other means.

3.2.4.2.3. In the event there is insufficient or out-of-date contract information for ten (10) or more individuals affected by a breach, such substitute notice shall:

3.2.4.2.3.1. Be in the form of either a conspicuous posting for a period of ninety (90) days where an individual can learn whether such individual's unsecured PHI may have been included in the breach.

3.2.4.2.3.2. Include a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether such individual's unsecured PHI may have been included in the breach.

3.2.4.3. Additional Notice in Urgent Situations: In any case deemed to require urgent notification due to possible imminent misuse of unsecured PHI, such Health Care Component may provide information to affected individuals by telephone or other means, as appropriate, in addition to any written notice as required under this Regulation.

3.3. Notification to the Media

3.3.1. Requirement

In the event of a breach of unsecured PHI involving more than five-hundred (500) residents of a State or jurisdiction, an ECU Health Care Component shall, without unreasonable delay and in no case later than sixty (60) calendar days after discovery of breach, notify prominent media outlets serving such State or jurisdiction.

3.3.2. Content of Notification

Any notification provided to the media pursuant to this Section shall contain all information as required under Article 3.2.3 above.

3.4. Notification to the Secretary of Health and Human Services

3.4.1. Requirement for breaches involving 500 or more individuals

In the event of a breach of unsecured PHI involving five-hundred (500) or more individuals, the University shall, except as provided in 42 C.F.R. Sect. 164.412 (Law Enforcement Delay), provide the notification to the Secretary of Health and Human Services ("HHS") in the manner specified by HHS at the time of such breach.

3.4.2. Requirement for breaches involving less than 500 individuals

In the event of a breach of unsecured PHI involving fewer than five-hundred (500) individuals, the University shall maintain a log or other documentation of such breaches and, not later than sixty (60) days following the end of each calendar year, provide notification to HHS of breaches discovered during the preceding calendar year, in the manner specified by HHS at the time of such required reporting.

3.5. Application of Other ECU HIPAA Privacy Regulations

3.5.1. Training regarding this Regulation shall be provided as set

forth in the ECU HIPAA Training, ECU REG 12.60.06.

3.5.2. Complaints regarding failure to comply with this Regulation may be issued pursuant to Privacy Complaint Process, ECU REG 12.60.08.

3.5.3. Sanctions against members of the workforce of any ECU Health Care Component for failure to comply with this Regulation shall be applied as set forth in Sanctions, REG 12.60.07.

3.6. Institutional Determination of Whether Notification is Required under this Regulation

3.6.1. Once it has been determined by the ECU HIPAA Privacy Officer that there has been an impermissible accession, use, or disclosure of PHI by an individual according to the HIPAA Privacy Rules, the ECU HIPAA Privacy Office shall conduct a risk assessment to determine whether any notification or reporting of such use or disclosure of PHI is required pursuant to this Regulation.

3.6.2. In the event the ECU HIPAA Privacy Office determines that notification is required under this Regulation, such notification shall be performed by the ECU HIPAA Privacy Office.

3.6.2.1. In the event the ECU HIPAA Privacy Office determines that notification is not required, the ECU HIPAA Steering Committee shall conduct an additional risk assessment to confirm or reject the determination of the HIPAA Privacy Officer.

3.6.2.2. In the event the ECU HIPAA Privacy Office is unable to definitively whether notification is required under this regulation, the ECU HIPAA Steering Committee shall conduct the risk assessment to definitively determine whether any notification or reporting of such use or disclosure of PHI is required.

3.6.3. The ECU HIPAA Privacy Office shall be responsible to provide any notification to HHS that may be required under this Regulation.

3.7 Coordination with the ECU Identify Theft Protection Committee

3.7.1 If the unsecured PHI that was Breached includes Personal Identifying Information, as defined by N.C. Gen. Stat. § 75-61 to -66,

the ECU HIPAA Privacy Office will notify the IT Security Officer.