HIPAA Sanctions

REG12.60.07 Current Version

Authority: Chancellor

History: Effective: September 19, 2013; Revised: January 8, 2004; July 24, 2006; December 6, 2007; October 8, 2010; September 18, 2013; Transitioned from Interim to Permanent: July 17, 2014. Revised and approved as Interim February 4, 2015. Current version transitioned from Interim to Permanent July 31, 2015.

Related Policies:

Additional Resources: 45 CFR 164 Subpart E: Privacy of Individually Identifiable Health Information
"Modification to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," 78 Federal Register 17 (25 January 2013), pp. 5566-5702.
ECU Healthcare Components

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

Archived Versions:
Version 1 Version 2 Compare Versions

1. Purpose

1.1. East Carolina University's Health Care Components ("ECU's Health Care Components") have a duty to protect the privacy of protected health information ("PHI"). The purpose of this regulation is to define the violation levels and sanctions for noncompliance with ECU's HIPAA privacy and security regulations.

2. Definitions

2.1. Disclosure means the release, transfer, provision of access to, or divulging in any manner of PHI outside of an ECU Health Care Component. This includes PHI from Vidant Medical Center or any other covered entity to which a Workforce member has access by virtue of their Workforce status with ECU.

2.2. Protected Health Information means:

2.2.1. Individually identifiable information, that is a subset of health information, including demographic information collected from an individual, and:

2.2.1.1. (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2.2.1.2. (2) relates to the past, present, or future physical or mental health or condition of a subject; the provision of health care to a subject; or the past, present, or future payment for the provision of health care to a subject; and

2.2.1.2.1. That identifies the subject; or

2.2.1.2.2. With respect to which there is reasonable basis to believe the information can be used to identify the individual.

2.2.2. PHI can be:

2.2.2.1. Transmitted by electronic media;

2.2.2.2. Maintained in electronic media; or

2.2.2.3. Transmitted or maintained in any other form or medium.

2.2.3. PHI excludes individually identifiable information that is:

2.2.3.1. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20. U.S.C. 1232g;

2.2.3.2. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

2.2.3.3. In employment records held by a covered entity in its role as employer; and

2.2.3.4. Regarding a person who has been deceased for more than 50 years.

2.3. Use means the sharing, employment, application, utilization, examination, or analysis of PHI within ECU's Health Care Components.

2.4. Workforce means employees, volunteers, trainees, learners, faculty, students and other persons whose conduct in the performance of work for an ECU Health Care Component, is under the direct control of such ECU Health Care Component, whether or not they are paid by the ECU Health Care Component.

3. Regulation

3.1. It is the policy of ECU to have and apply appropriate sanctions against members of its Workforce who fail to comply with ECU's privacy regulations and procedures to protect the confidentiality and security of PHI.

3.2. Sanctions will be imposed based on the severity of the violation, whether it was intentional or unintentional, and whether the violation indicated a pattern or practice of improper Use or Disclosure. The following violation levels outline some, but not all, types of violations that may occur:

3.2.1. Level 1 : Failure to demonstrate appropriate care and safeguards in handling PHI. These are usually unintentional with no improper exposure of the information. Examples of Level 1 violations may include failing to log-off of a system, leaving PHI unattended in a non-secure area, or other minor first-time violations of regulations.

3.2.2. Level 2 : Intentional or unintentional exposure of PHI or internal inappropriate access, unauthorized access to PHI, or repeated Level 1 violations. These result in no improper further exposure inside an ECU Health Care Component or no Disclosure outside of an ECU Health Care Component or, if applicable, the University setting. Examples of Level 2 violations may include sharing ID/passwords with other staff that result in internal inappropriate access, accessing PHI for which the individual has no responsibility or which is needed as part of

assigned duties.

3.2.3. Level 3 : Intentional or unintentional exposure of PHI inside an ECU Health Care Component or Disclosure outside of an ECU Health Care Component or, if applicable the University setting, or repeated Level 2 violations. Examples of Level 3 violations may include providing passwords to unauthorized individuals that result in a Disclosure outside ECU's Health Care Components, sharing of PHI with unauthorized individuals, and failing to perform the necessary responsible actions that would prevent disclosure of PHI.

3.2.4. Level 4 : Intentional Abuse of PHI. Examples of Level 4 violations may include large-scale disclosures of PHI, using PHI for personal gain, or altering, tampering with, or destroying PHI.

3.3. Sanctions for members of the Workforce include documented performance counseling up to dismissal depending on the level of violation and management's consideration of all relevant factors. Violations and recommended sanctions are:

3.3.1. Staff (SPA/CSS Employees):

3.3.1.1. Level 1 Violations : Documented performance counseling and warning by the first line supervisor in accordance with East Carolina University's Disciplinary Policies and Procedures for State Personnel Act (SPA) and Clinical Support Services (CSS) employees.

3.3.1.2. Level 2 Violations : First line supervisor and next immediate manager work with the Department of Human Resources to initiate a Written Warning in accordance with East Carolina University's Disciplinary Policies and Procedures for State Personnel Act (SPA) and Clinical Support Services (CSS) employees.

3.3.1.2.1 If the exposure of PHI is the result of a minor lapse or oversight by the employee (e.g. keyboard error); and does not involve highly sensitive PHI, a large amount of PHI or present a significant level of risk to the patient (If a question arises to the level of risk, the first line supervisor and representative from Human Resources shall consult with the HIPAA Privacy Office.) then the Department of Human Resources and the first line supervisor responsible for operations in the department may together determine that a coaching/education session is a sufficient penalty for the violation. This coaching/education session shall include at minimum: a full review of the incident; the employees role;

discussions regarding potential mitigation; and the identification of appropriate preventative actions. If a formal coaching/education session is selected as the appropriate remedy, the first line supervisor responsible for such session will notify the ECU HIPAA Privacy Office when that session is complete; d. The option of a formal coaching/education session should not be used when the employee has committed the same offense multiple times.

3.3.1.3. Level 3 Violations : Most senior staff member directly responsible for operations works with the Department of Human Resources to initiate a Written Warning or formal disciplinary action up to and including dismissal in accordance with East Carolina University's Disciplinary Policies and Procedures for State Personnel Act (SPA) and Clinical Support Services (CSS) employees.

3.3.1.3.1 If the exposure of PHI is the result of a minor lapse or oversight by the employee (e.g. keyboard error); and does not involve highly sensitive PHI, a large amount of PHI or present a significant level of risk to the patient (If a question arises to the level of risk, the senior staff member and representative from Human Resources shall consult with the HIPAA Privacy Office.) then the Department of Human Resources and the most senior staff member responsible for operations in the department may together determine that a coaching/education session is a sufficient penalty for the violation. This coaching/education session shall include at minimum: a full review of the incident; the employees role; discussions regarding potential mitigation; and the identification of appropriate preventative actions. If a formal coaching/education session is selected as the appropriate remedy, the senior staff member responsible for such session will notify the ECU HIPAA Privacy Office when that session is completed. The option of a formal coaching/education session should not be used when the employee has committed the same offense multiple times.

3.3.1.4. Level 4 Violations - Most senior staff member responsible for overall operations works with the Department of Human Resources to initiate dismissal in accordance with East Carolina University's Disciplinary Policies and Procedures for State Personnel Act (SPA) and Clinical Support Services (CSS) employees. Other departmental resources may be included to assist at his/her discretion.

3.3.2. University Faculty and Exempt from Personnel Act (EPA) Employees:

3.3.2.1. Level 1 Violations : Documented performance counseling and warning by the person with immediate supervisory responsibilities.

3.3.2.2. Level 2 Violations : Documented performance counseling and warning from the appropriate Dean and Vice Chancellor. Further actions may be initiated per University policies and procedures for Teaching and Non-Teaching Exempt from the Personnel Act employees.

3.3.2.3. Level 3 Violations : Referral to the Vice Chancellor with supervisory authority for possible initiation of disciplinary actions per University policies and procedures for Teaching and Non-Teaching Exempt from the Personnel Act employees.

3.3.2.4. Level 4 Violations : Referral to the Vice Chancellor with supervisory authority for discharge or suspension per University policies and procedures for Teaching and Non-Teaching Exempt from the Personnel Act employees.

3.3.3. University Students (Non-Medical):

3.3.3.1. Level 1 Violations : Documented counseling by the appropriate program coordinator or Department Chair.

3.3.3.2. Level 2 Violations : Documented counseling by the appropriate Dean. The Dean may refer violations to the Vice Chancellor, Student Life or Student Attorney General for further actions per the Student Handbook, University Policies and Regulations.

3.3.3.3. Level 3 Violations : Referral to the Vice Chancellor, Student Life or Student Attorney General for penalties per the Student Handbook, University Policies and Regulations to include possible probation or suspension.

3.3.3.4. Level 4 Violations : Referral to the Vice Chancellor, Student Life or Student Attorney General for penalties per the Student Handbook, University Policies and Regulations for suspension or expulsion.

3.3.4. University Medical Students:

3.3.4.1. Level 1 Violations : Documented counseling by the Assistant Dean, Student Affairs.

3.3.4.2. Level 2 Violations : Documented counseling by the Assistant Dean, Student Affairs and Dean, Brody School of Medicine. Further actions per the Medical Student Handbook, Educational Policies of the Brody School of Medicine and Code of Student Conduct may be taken.

3.3.4.3. Level 3 Violations : Referral to the Assistant Dean, Student Affairs and the Dean, Brody School of Medicine for penalties per the Medical Student Handbook, Educational Policies of the Brody School of Medicine and Code of Student Conduct to include probation or suspension.

3.3.4.4. Level 4 Violations : Referral to the Assistant Dean, Student Affairs and the Dean, Brody School of Medicine for penalties per the Medical Student Handbook, Educational Policies of the Brody School of Medicine and Code of Student Conduct for suspension or expulsion.

3.4. Non ECU Employees and Students and ECU Visitors/Volunteers:

3.4.1. ECU will refer violation to the host institution or HIPAA Privacy Officer of the facility in which the infraction occurred.

3.5. Exceptions to Sanctions Requirement

3.5.1. Disclosures by Whistleblowers

3.5.1.1. ECU does not have to apply sanctions against a member of its Workforce who discloses PHI provided that:

3.5.1.1.1. The Workforce member believes in good faith that an ECU Health Care Component has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by ECU potentially endangers one or more patients, workers, or the public; and

3.5.1.1.2. The disclosure is to

3.5.1.1.2.1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of an ECU Health Care Component or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or

misconduct by a Component; or

3.5.1.1.2.2. An attorney retained by or on behalf of the Workforce member for the purpose of determining the legal options of the Workforce member with regard to the conduct described in paragraph 3.5.1.1.1.

3.5.2. Disclosures by Workforce Members who are Victims of a Crime

3.5.2.1. ECU does not have to apply sanctions to a member of its Workforce who is the victim of a criminal act and discloses PHI to a law enforcement official, provided that:

3.5.2.1.1. The PHI disclosed is about the suspected perpetrator of the criminal act; and

3.5.2.1.2. The PHI disclosed is limited to the purpose of identifying or locating a suspected perpetrator and can only include:

3.5.2.1.2.1. Name and address;

3.5.2.1.2.2. Date and place of birth;

3.5.2.1.2.3. Social security number;

3.5.2.1.2.4. ABO blood type and rh factor;

3.5.2.1.2.5. Type of injury;

3.5.2.1.2.6. Date and time of treatment;

3.5.2.1.2.7. Date and time of death, if applicable; and

3.5.2.1.2.8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

4. Procedure

4.1. Upon receiving report of a possible HIPAA violation, the ECU

HIPAA Privacy Officer will conduct a confidential investigation of the alleged violation.

4.1.1. If appropriate, the ECU HIPAA Privacy Officer will interview any person who may have knowledge of the alleged violation.

4.2. The ECU HIPAA Privacy Officer will determine if a violation has occurred in accordance with the violation levels outlined in paragraph 3.2.

4.2.1. If a violation has occurred, the decision will be documented in writing and sanctions will be applied in accordance with paragraph 3.3.