Faculty Senate Resolution #15-54
Approved by the Faculty Senate: April 14, 2015
Accepted by the Chancellor: May 12, 2015

Formal faculty advice on revised HIPAA Notification in the Event of a Breach of Unsecured Protected Health Information (PHI) Policy, revised Notification in the Event of Breach of Unsecured Protected Health Information Policy and revised HIPAA Sanctions Policy, as follows:

Formal Faculty Advice on Revised HIPAA Notification in the Event of a Breach of Unsecured Protected Health Information (PHI) Policy

No revisions are being recommended to this revised policy.

History: September 19, 2013Revised: February 2, 2010; October 12, 2010; September 18, 2013Transitioned from Interim to Permanent: July 17, 2014.

Related Policies:
ECU HIPAA Training
Privacy Complaint Process
Sanctions

Additional References:
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

---

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.

Formal Faculty Advice on Revised Notification in the Event of Breach of Unsecured Protected Health Information Policy

No revisions are being recommended to this revised policy.

Authority: Board of Trustees
History: Effective: September 23, 2009
Revised: February 2, 2010
October 12, 2010
[enter new revision date]
Additional References:
(45 CFR 164 Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information – http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=34e701754473b94a5b572a6e9438921f&rgn=div6&view=text&node=45:1.0.1.3.78.4&idno=45)

(Department of Health & Human Services – Breach of Unsecured Personal Health Information – http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/)
(ECU Healthcare Components – http://www.ecu.edu/cs-dhs/hipaa/privacy/upload/2012-Health-Care-Components.pdf)
(Guidelines for Media Sanitization – http://www.csrc.nist.gov/)

Contact for Info: ECU HIPAA Privacy Office, 252-744-5200

---

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 policy 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 Policy.

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 Policies

3.5.1. Training regarding this Policy shall be provided as set forth in the HIPAA Privacy Policy #0018.

3.5.2. Complaints regarding failure to comply with this Policy may be issued pursuant to HIPAA Privacy Policy #0003.

3.5.3. Sanctions against members of the workforce of any ECU Health Care Component for failure to comply with this Policy shall be applied as set forth in ECU HIPAA Privacy Policy #0002.

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

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 Steering Committee shall conduct a risk assessment to determine whether any notification or reporting of such use or disclosure of PHI is required pursuant to this Policy.

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

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

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.

Formal Faculty Advice on Revised HIPAA Sanctions

No revisions are being recommended to this revised policy.

History: September 19, 2013
Revised: January 8, 2004; July 24, 2006; December 6, 2007; October 8, 2010; September 18, 2013Transitioned from Interim to Permanent: July 17, 2014.

Related Policies:

Additional References:
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

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 employee's 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 completed. The option of a formal coaching/education session should not be used when the employee has committed the same offense multiple times.

3.3.1.3. 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 employee's 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.