East Carolina University
HIPAA Security Standards

Subject: Termination Procedures
Coverage: ECU Health Care Components
Standard #: Security-0003c
Page: 1 of 3
Supersedes:
Page: 1 of 3
Effective Date: April 21, 2005
Review Date: May 30, 2013

HIPAA Security Rule Language: “Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.”

Regulatory Reference: 45 CFR 164.308(a)(3)(ii)(C)

I. PURPOSE

This standard reflects East Carolina University’s commitment to create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

II. AUTHORIZATION AND ENFORCEMENT

Health Care component management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the ECU IT Security Officer, ECU HIPAA Security Officer, and ECU HIPAA Privacy Officer.

III. STANDARD

When the employment of ECU Health Care Component workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. When workforce members depart from ECU, they must return all ECU supplied equipment by the time of departure. A workforce member who departs from ECU must not retain, give away, or remove from ECU premises any ECU information. Special attention must be paid to situations where a workforce member has been terminated and poses a risk to information or systems at ECU.
IV. APPLICABILITY

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI which is shared across the network and accessed by healthcare workers.

V. PROCEDURE

The following standards and safeguards must be implemented to satisfy the requirements of this standard:

1. ECU Health Care Components must create and implement a formal, documented process for terminating access to EPHI when the employment of a workforce member ends.

2. When the employment of ECU Health Care Component workforce members ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. Consideration should also be given to physical access to areas where EPHI is located.

3. All ECU Health Care Component workforce members must have their information system privileges automatically disabled after their user ID or access method has had 60 days of inactivity. All such privileges that are disabled in this manner must be reviewed to ensure that the inactivity is not due to termination of employment. If termination is the reason for inactivity, there must be review of situation to ensure that all access to EPHI (or ability to physically access information) has been eliminated.

4. When workforce members depart from ECU, they must return all ECU supplied equipment (PCs, PDAs, OneCard, Keys, etc.) by the time of departure. The return of all such equipment must be tracked and logged.

5. If a departing workforce member has used cryptography on ECU data, they must make the cryptographic keys available to appropriate management by the time of departure.

6. As appropriate, all physical security access codes used to protect ECU information systems that are known by a departing workforce member must be deactivated or changed. For example, the PIN to a keypad lock that restricts entry to an ECU facility containing information systems with EPHI must be changed if a workforce member who knows the PIN departs.

7. A workforce member who departs from ECU must not retain, give away, or remove from ECU premises any ECU information (this does not apply to copies of information provided to the public or copies of correspondence directly related to the terms and conditions of employment). All other ECU information in the possession of the departing
workforce member must be provided to the person's immediate supervisor at the time of departure.

8. Prior to the departure of a terminating ECU Health Care Component workforce member, their computers’ resident files must be promptly reviewed by their immediate supervisors to determine the appropriate transfer or disposal of any confidential information.

9. Special attention must be paid to situations where a departing employee poses a risk to information or systems at ECU. If a workforce member is to be terminated immediately, their information system privileges must be removed or disabled just before they are notified of the termination.

10. Health Care Components or their designees must periodically review information system access privileges to ensure that this policy is being adhered to and that existing procedures are effective.

VI. COORDINATING INSTRUCTIONS

1. All section policies, standards and procedures will be reviewed annually. Every section policy, standard and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention.