HIPAA Security Standards

<table>
<thead>
<tr>
<th>Subject:</th>
<th>Access Establishment and Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage:</td>
<td>ECU Health Care Components</td>
</tr>
<tr>
<td>Standard #:</td>
<td>Standard-0004b</td>
</tr>
<tr>
<td>Page:</td>
<td>1 of 3</td>
</tr>
<tr>
<td>Supersedes:</td>
<td></td>
</tr>
<tr>
<td>Effective Date:</td>
<td>April 21, 2005</td>
</tr>
<tr>
<td>Review Date:</td>
<td>May 30, 2013</td>
</tr>
</tbody>
</table>

HIPAA Security Rule Language:

“Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.”

Regulatory Reference:

45 CFR 164.308(a)(4)(ii)(B)

I. PURPOSE

This standard reflects East Carolina University’s commitment to have a formal documented process for establishing, documenting, reviewing, and modifying access to ECU information systems containing EPHI.

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

ECU Health Care Components must have a formal, documented process for establishing, documenting, reviewing, and modifying access to ECU information systems containing EPHI.

Authorized ECU information system owners/stewards or their designated delegates must regularly review workforce member access rights to ECU information systems containing EPHI to ensure that they are provided only to those having a need for specific information in order to accomplish a legitimate task. All revisions to ECU workforce member access rights must be tracked and logged. Reviews should be accomplished at
intervals that meet the Statewide Information Security Standards, and other applicable governing directives.

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 safeguards must be implemented to satisfy the requirements of this standard:

1. ECU Health Care Components must have a formal, documented process for establishing, documenting, reviewing, and modifying access to ECU information systems containing EPHI. At a minimum, the process must include:

   - Procedure for establishing different levels of access to ECU information systems containing EPHI.
   - Procedure for documenting levels of access established to ECU information systems containing EPHI.
   - Procedure for regularly reviewing ECU workforce member access privileges to ECU information systems containing EPHI. Reviews should be accomplished at intervals that meet the Statewide Information Security Standards, and other applicable governing directives.
   - Procedure for modifying ECU workforce member access privileges to ECU information systems containing EPHI.

2. Only properly authorized and trained ECU workforce members may access ECU information systems containing EPHI. Such access must be established via a formal, documented process. At a minimum, this process must include:

   - Identification and definition of permitted access methods
   - Identification and definition of length of time that access will be granted
   - Procedure for both granting a workforce member an access method (e.g. password or token) and changing an existing access method
   - Procedure for managing access rights in a distributed and networked environment
   - Appropriate tracking and logging of activities by authorized workforce members on ECU information systems containing EPHI

3. Where appropriate, security controls or methods that allow access to be established to ECU information systems containing EPHI must include, at a minimum:
• Unique user identifiers (user IDs) that enable individual users to be uniquely identified. User IDs must not give any indication of the user’s privilege level. Common or shared identifiers must not be used to gain access to ECU information systems containing EPHI. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to ECU information systems not containing EPHI. However, this should be a last resort when there are no other feasible alternatives. Further, anytime shared identifiers are used, the system and/or applicable administrators and data owners must have a mechanism of tracking the individuals that are aware of the shared identifiers/credentials. The shared identifiers/credentials must be changed promptly anytime an individual with knowledge of the credentials and passphrase transfers or is terminated from employment by the University, or no longer needs access to the EPHI for any reason.
• The prompt removal or disabling of access methods for persons and entities that no longer need access to ECU EPHI.
• Verification that redundant user identifiers are not issued.

4. Access to ECU information systems containing EPHI must be limited to ECU workforce members who have a need for specific EPHI in order to perform their job responsibilities.

5. Appropriate ECU information system owners/stewards or their designated delegates must regularly review workforce member access rights to ECU information systems containing EPHI to ensure that they are provided only to those who have a need for specific EPHI in order to accomplish a legitimate task. Such rights must be revised as necessary. Reviews should be accomplished at intervals that meet the Statewide Information Security Standards, and other applicable governing directives.

6. All revisions to ECU workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information:

- Date and time of revision
- Identification of workforce member whose access is being revised
- Brief description of revised access right(s)
- Reason for revision

This information must be securely maintained.

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.