East Carolina University
HIPAA Security Standard

<table>
<thead>
<tr>
<th>Subject:</th>
<th>Response and Reporting</th>
<th>Coverage:</th>
<th>ECU Health Care Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard #:</td>
<td>Security-0006a</td>
<td>Page:</td>
<td>1 of 2</td>
</tr>
<tr>
<td>Supersedes:</td>
<td></td>
<td>Approved:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td>May 30, 2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HIPAA Security Rule Language:
“Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.”

Regulatory Reference: 45 CFR 164.308(a)(6)(ii)

I. PURPOSE
This standard reflects East Carolina University’s commitment to effectively detect and respond to security incidents in order to protect the confidentiality, integrity, and availability of its information systems.

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 be able to effectively detect, respond to, and mitigate the effects of security incidents in order to protect the confidentiality, integrity, and availability of its EPHI stored on healthcare computing systems.

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 policy:

1. ECU Health Care Components must have process for detecting security incidents. This may include, but is not limited to: regular review of data access logs, system alert messages, and other application anomalies.

2. ECU Health Care Components must report suspected security incidents to the University Help Desk.

3. ECU Health Care Components must document the security incident, which includes at a minimum the following:
   - Name of person(s) conducting the incident response investigation
   - Description of the data and the computing system affected by the incident
   - Time and date of incident
   - Damage to data and the computing system(s)
   - Suspected cause of the incident
   - Actions taken to mitigate damage and restore the data and/or computing system
   - Recommendations for further actions to enhance security of EPHI

4. ECU Health Care Components must submit incident documentation to the IT Security Officer.

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.