East Carolina University
HIPAA Security Standards

<table>
<thead>
<tr>
<th><strong>Subject:</strong> Mechanism to Authenticate Electronic Protected Health Information</th>
<th><strong>Coverage:</strong> ECU Health Care Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard #:</strong> Standard-0013a</td>
<td><strong>Page:</strong> 1 of 2</td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
<td><strong>Approved:</strong></td>
</tr>
<tr>
<td><strong>Effective Date:</strong> April 21, 2005</td>
<td><strong>Revised:</strong> December 9, 2010, April 12, 2012, May 30, 2013</td>
</tr>
<tr>
<td><strong>Review Date:</strong> May 30, 2013</td>
<td></td>
</tr>
</tbody>
</table>

**HIPAA Security Rule Language:** “Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.”

**Regulatory Reference:** 45 CFR 164.312(c)(2)

I. PURPOSE

This standard reflects East Carolina University’s commitment to implement appropriate electronic mechanisms to confirm that electronic EPHI contained on ECU healthcare computing systems has not been altered or destroyed in an unauthorized manner.

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 implement appropriate electronic mechanisms to confirm that EPHI contained on ECU healthcare computing systems has not been altered or destroyed in an unauthorized way.

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

1. Electronic mechanisms used to protect the integrity of EPHI contained on ECU healthcare computing systems must ensure that the value and state of the EPHI is maintained, and it is protected from unauthorized modification and destruction. Such mechanisms must also be capable of detecting unauthorized alteration or destruction of EPHI. Such mechanisms might include:

   - System memory, hard drives, and other data storage devices with error-detection capabilities
   - File and data checksums
   - Encryption

VI. COORDINATING INSTRUCTIONS

1. All section policies and procedures will be reviewed annually. Every section policy 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 period.