East Carolina University
HIPAA Security Policies

Subject: Contingency Plan
Coverage: ECU Health Care Components
Policy #: Security-0007
Page: 1 of 2
Supersedes:
Approved:
Effective Date: April 21, 2005
Review Date: May 30, 2013

HIPAA Security Rule Language: “Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (EPHI).”

Regulatory Reference: 45 CFR 164.308(a)(7)(i)

I. PURPOSE

This policy reflects East Carolina University’s commitment to effectively prepare for and respond to emergencies or disasters 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. POLICY

ECU Health Care Components must have a formal process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems.

ECU’s disaster and emergency response process must reduce the disruption to ECU information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to ECU information systems, limit damage caused by disasters and emergencies, and ensure the timely resumption of significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.
ECU workforce members must receive regular training and awareness on the university’s disaster preparation and disaster and emergency response processes.

IV. APPLICABILITY

This policy 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 a formal process for assuring all EPHI on the University’s information systems and electronic media must be regularly backed up and securely stored as specified in the Data Backup Standard.

2. ECU Health Care Components must create and document a Disaster Recovery Plan to recover its information systems if they are impacted by a disaster as specified in the Disaster Recovery Plan Standard.

3. ECU Health Care Components must have a formal, documented Emergency Mode Operations plan to enable the continuance of crucial business processes that protect the security of its information systems containing EPHI during and immediately after a crisis situation as specified in the Emergency Mode Operations Plan Standard.

4. ECU Health Care Components must conduct regular testing of its Disaster Recovery Plan to ensure that it is up to date and effective as specified in the Testing and Revision Procedures Standard.

5. ECU Health Care Components must have a formal process for defining and identifying the criticality of its information systems as specified in the Application and Data Criticality Analysis Standard.

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 period.