

Policies and Procedures

<i>SECTION:</i> Administration	<i>NO.</i> 2.4.17.		
<i>CHAPTER:</i> Information Technology	<i>ISSUED:</i> 4/7/06	<i>REV. A</i>	<i>REV. B</i>
<i>POLICY:</i> Emergency Mode of Operation Policy	<i>PAGE 1 OF 2</i>		

PURPOSE

The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to its response to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI).

SCOPE

The scope of this Policy contains procedures regarding a contingency plan that shall be developed and implemented in the event of an emergency, disaster or other occurrence (i.e. fire, vandalism, system failure and natural disaster) when any system that contains electronic protected health information (ePHI) is affected, including data backup, disaster recovery planning and emergency mode operation plan. This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy applies to all faculty, staff, students, residents, postdoctoral fellows, and non-employees (including visiting faculty, courtesy, affiliate, and adjunct faculty, industrial personnel, and others) who collect, maintain, use, or transmit ePHI in connection with activities at Creighton University.

POLICY

Creighton University requires that an Emergency Mode Operation Plan be developed and implemented to enable continuation of critical business processes and to protect the security of ePHI while operating in emergency mode.

Emergency mode operation procedures detailed in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

DEFINITIONS

Protected Health Information

Individually identifiable health information transmitted or maintained in any form.

Electronic Protected Health Information (ePHI)

Individually identifiable health information transmitted or maintained in electronic form.

Emergency Mode of Operation Plan

Procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in an emergency mode.

RESPONSIBILITIES

Network administrators are responsible for the creation, maintenance, and implementation of the disaster recovery plan for each system that collects, maintains, uses or transmits ePHI.

Policies and Procedures

SECTION: Administration	NO. 2.4.17.		
CHAPTER: Information Technology	ISSUED: 4/7/06	REV. A	REV. B
POLICY: Emergency Mode of Operation Policy	PAGE 2 OF 2		

Information Security Officer is responsible for ensuring each system that collects, maintains, uses or transmits ePHI has a documented disaster recovery plan that is tested periodically.

ADMINISTRATION AND INTERPRETATIONS

This policy shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE POLICIES

HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/>, February 20, 2003.

EXCEPTIONS

None

VIOLATIONS/ENFORCEMENT

Any known violations of this policy should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.