

# *Policies and Procedures*

<i>SECTION:</i> <b>Administration</b>	<i>NO.</i> <b>2.4.28.</b>		
<i>CHAPTER:</i> <b>Information Technology</b>	<i>ISSUED:</i> 4/7/06	<i>REV. A</i>	<i>REV. B</i>
<i>POLICY:</i> <b>Accountability Policy</b>	<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 the integrity, confidentiality, and availability of electronic protected health information. This policy intends to

## **SCOPE**

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 (CU).

## **POLICY**

Creighton University requires that a record be maintained to identify movements of ePHI-related hardware and devices. The movement of hardware, electronic media and devices includes the receipt, removal, storage and/or disposal of ePHI systems. Such information will also include the identity of responsible persons associated with the movement.

Movements of mobile hardware, media, or devices does not have to be tracked, but ownership of this equipment must be recorded.

## **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.

### **Electronic Device**

In this policy, electronic devices are workstations, PDAs, laptops, tablet PCs, USB Flash drives, backup media, floppy disks, removable hard drives, or any other device that has the capability to store, access, or transmit ePHI.

## **RESPONSIBILITIES**

**All individuals identified in the scope of this policy** are responsible for compliance with this policy

**Systems Administrators** are responsible for implementing procedures to track the movement of hardware, media, and devices that contain ePHI.

**Information Security Officer** is responsible for verifying the adherence of this policy.

# ***Policies and Procedures***

<b>SECTION:</b> <b>Administration</b>	<b>NO.</b> <b>2.4.28.</b>		
<b>CHAPTER:</b> <b>Information Technology</b>	<b>ISSUED:</b> 4/7/06	<b>REV. A</b>	<b>REV. B</b>
<b>POLICY:</b> <b>Accountability Policy</b>	<b>PAGE 2 OF 2</b>		

## **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](mailto: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.