Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.26.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A*	*REV. B*
POLICY: **Workstation Security Policy**	*PAGE 1 OF 2*		

PURPOSE

The purpose is to implement physical safeguards for all workstations that access electronic protected health information (ePHI) and to restrict access to authorized users.

SCOPE

This policy applies to all Creighton University workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by Creighton University. In addition, this policy applies to all workstations and other computing devices owned or operated by Creighton University and any computing device that connects to Creighton University's internal network.

POLICY

Creighton University requires reasonable physical safeguards be implemented for all workstations and other electronic devices that access ePHI. Physical safeguards should reasonably prevent the theft of or unauthorized access to electronic devices that access, store, or transmit ePHI. Physical safeguards must be implemented where ever the electronic devices exist.

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.

Physical Safeguards
Electronic or mechanical mechanisms that are used to reasonably prevent the theft or physical access to electronic devices.

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.

Distributed PC Technician
The individual that is responsible for the support of a specific area's personal computers. Support may be handled by local employees of a department or handled by the Division of Information Technology (DoIT).

RESPONSIBILITIES

Covered entity's workforce is responsible for following all procedures implemented in relation to this policy.

Distributed PC Technicians are responsible for ensuring the workstations under their realm of responsibility that access ePHI are reasonably protected to prevent the theft of or unauthorized access to electronic devices that access, store, or transmit ePHI.

Information Security Officer is responsible for verifying that reasonable protective measures have been implemented.

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.