Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.12.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A*	*REV. B*
POLICY: **Log-in Monitoring Policy**	*PAGE 1 OF 2*		

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 (ePHI).

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.

POLICY

To ensure that access to servers, workstations, and other computer systems containing PHI is appropriately secured; Creighton University will configure all critical components that process, store or transmit ePHI to record log-in attempts – both successful and unsuccessful – as well as automatic lock out and reporting after 3 failed attempts.

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.

Log-in Monitoring
The process of logging or recording all successful and unsuccessful log-in attempts in order to monitor or hacking or other inappropriate activity.

Automatic Lock Out
The process of locking an account after a predetermined number of unsuccessful login attempts.

RESPONSIBILITIES

Network users are responsible for understanding and consenting to Creighton University’s use of tools and processes to monitor system activity.

Administrators of systems that maintain PHI are responsible for ensuring the policies statements detailed above are implemented on all systems that store, transmit, or maintain PHI.

Policies and Procedures

SECTION: **Administration**	***NO.*** **2.4.12.**		
CHAPTER: **Information Technology**	***ISSUED:*** 4/7/06	*REV. A*	*REV. B*
POLICY: **Log-in Monitoring Policy**	*PAGE 2 OF 2*		

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.