

Policies and Procedures

<i>SECTION:</i> Administration	<i>NO.</i> 2.4.34.		
<i>CHAPTER:</i> Information Technology	<i>ISSUED:</i> 4/7/06	<i>REV. A</i>	<i>REV. B</i>
<i>POLICY:</i> Audit Controls 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 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

Creighton University will identify critical systems that require event auditing capabilities. At a minimal, event auditing capabilities will be enabled on all systems that process, transmit, and/or store ePHI. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications.

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.

Event Auditing

The process of logging systems transactions to provide evidence of when transactions take place and who performed the transactions.

RESPONSIBILITIES

Systems Administrators are responsible for identifying systems that must have auditing enabled, implementing such auditing, and review and secure storage of said logs.

Information Security Officer is responsible for validating the University's adherence to this policy.

ADMINISTRATION AND INTERPRETATIONS

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

Policies and Procedures

SECTION: Administration	NO. 2.4.34.		
CHAPTER: Information Technology	ISSUED: 4/7/06	REV. A	REV. B
POLICY: Audit Controls Policy	PAGE 2 OF 2		

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.