

Policies and Procedures

SECTION: Administration	NO. 2.4.23.		
CHAPTER: Information Technology	ISSUED: 4/7/06	REV. A	REV. B
POLICY: Access Control 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

Creighton University will control access to its information assets and systems. Only individuals that have been formally authorized to view or change sensitive information will be granted access to that information.

The fundamental principal of "need to know" will be applied within Creighton University to determine access privileges. Access to ePHI will be granted only if that individual has a legitimate need for the information. Reasonable efforts will be made to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

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.

RESPONSIBILITIES

Systems Administrators are responsible for determining who needs physical access to the systems that maintain, transmit, or process ePHI.

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. 2.4.23.		
CHAPTER: Information Technology	ISSUED: 4/7/06	REV. A	REV. B
POLICY: Access Control 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.