Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.8.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A*	*REV. B*
POLICY: **Access Authorization 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

System Administrators who are responsible for systems that collect, maintain, use or transmit ePHI will grant access to system users following a formal request made by the supervisor of the specific user and/or data owner. Access to the system(s) will be limited to specific, defined, documented and approved applications and levels of access rights.

DEFINITIONS

Protected Health Information (PHI)
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.

Data Owner
The individual responsible for the policy and practice decisions of data.

RESPONSIBILITIES

System Users are responsible for adhering to the standards outlined in this policy when using Creighton University's Systems that contain e-PHI.

System Administrators are responsible for granting the appropriate access to users requesting access and for requiring authorization from supervisors/data owners before granting access.

Supervisors are responsible for requesting access from the appropriate system administrator for the users that they supervise.

Information Security Officer is responsible for verifying that the established access authorization controls are sufficient for each system and application that maintains ePHI and that the process has been implemented in an effective manner.

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.