Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.39.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A*	*REV. B*
POLICY: **Network Security Standard Policy**	*PAGE 1 OF 2*		

PURPOSE

The purpose of this policy is to protect the confidentiality and integrity of sensitive information such as electronic protected health information (ePHI) that may be sent or received via email.

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.

STANDARD

The standard for network protocols in Creighton's infrastructure is TCP/IP.

Creighton University will:

- Use encryption as much as possible to protect data
- Use firewall(s) to secure critical segments
- Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) on all critical segments
- Disable all services that are not in use or services that have use of which you are not sure

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

Information Security Officer is responsible for the creation of procedures required to support this policy and for supporting and ensuring compliance by workforce members.

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.