

# ***Policies and Procedures***

<b>SECTION:</b> <b>Administration</b>	<b>NO.</b> <b>2.4.1.</b>		
<b>CHAPTER:</b> <b>Information Technology</b>	<b>ISSUED:</b> 4/7/06	<b>REV. A</b>	<b>REV. B</b>
<b>POLICY:</b> <b>Risk Analysis Policy</b>	<b>PAGE 1 OF 2</b>		

## **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 requires systems administrators of systems that store, access, transmit, manipulate, input, or output Protected Health Information conduct a regular, accurate, and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. An assessment must be conducted before a new system goes into production or as material changes are made to existing systems.

## **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 adhering 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***

<b>SECTION:</b> <b>Administration</b>	<b>NO.</b> <b>2.4.1.</b>		
<b>CHAPTER:</b> <b>Information Technology</b>	<b>ISSUED:</b> 4/7/06	<b>REV. A</b>	<b>REV. B</b>
<b>POLICY:</b> <b>Risk Analysis Policy</b>	<b>PAGE 2 OF 2</b>		

## **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.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, 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](mailto: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.