# *Policies and Procedures*

| *SECTION:* **Administration** | *NO.* **2.4.36.** | | |
|---|---|---|---|
| *CHAPTER:* **Information Technology** | *ISSUED:* 4/7/06 | *REV. A* | *REV. B* |
| *POLICY:* **Person or Entry Authentication 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**

To ensure that all individuals or entities that access ePHI have been appropriately authenticated the following procedures must be implemented:

- Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.
- Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.
- Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.
- A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting EPHI.

**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.

**Workforce Member**
Any Staff, Faculty, Student, or designated 3rd party resource that works with ePHI

## RESPONSIBILITIES

**Network users** are responsible for adhering to this policy.

**Administrators of systems that maintain PHI** are responsible for ensuring the policies statements detailed above are implemented on all systems that store, transmit, or maintain PHI.

**Information Security Officer** is responsible for verifying that an authentication mechanism on systems that store, transmit, or maintain PHI are functional, appropriate and reasonably mitigate the risk of unauthorized access.

## 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.