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

Creighton University recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. Creighton will evaluate emerging encryption solutions for email and implement them when one is found that is:

- Technically sound
- Reasonable to implement and use by workforce members
- Financially reasonable

Until a workable encryption mechanism is implemented, Creighton University will utilize the following guidelines regarding sending PHI information via email:

- Emails containing sensitive information are permitted only when both the sender and receiver are members of Creighton’s workforce and the e-mail stays within the confines of Creighton’s local network. That is, both email addresses must end with “creighton.edu”. When sending ePHI via email, care should be taken to send only the minimum necessary.
- Emails containing sensitive information may not be sent to any other person outside of Creighton’s network or email address ending in anything other than “creighton.edu”.

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
**Covered entity's workforce** is responsible for following all procedures implemented in relation to this policy.

**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**


**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.