PURPOSE

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information.

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 (CU).

POLICY

Creighton University requires that prior to disposal or reuse of hardware or media that contains or previously contained ePHI either the data will be securely overwritten or the device and/or media be physically destroyed and that such steps taken will be documented.

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.

Securely Overwritten
The process of overwriting data with 1 and 0 to render the data irretrievable.

Physically Destroyed
The process of physically destroying electronic media to an extent where data is not longer retrievable.

Reuse of Hardware
The process of reallocating hardware that contains or may have contained ePHI to and individual that does not have authority to access ePHI.

RESPONSIBILITIES

All individuals identified in the scope of this policy are responsible for compliance with this policy.
MEDIA DISPOSAL AND RE-USE POLICY

SECTION: Physical Safeguards

CHAPTER: Device and Media Controls

POLICY: Media Disposal and Re-use Policy

Systems Administrators are responsible for following this policy when retiring, reallocating, or donating electronic media.

Information Security Officer is responsible for developing a University wide procedure for the secure disposal of electronic media.

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.