# 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 will appropriately discipline employees and other workforce members for any violation of security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and other disciplinary action in accordance with University procedures.

In addition, workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual’s information are subject to criminal investigation and prosecution or civil monetary penalties.

Creighton University will investigate any security incidents or violations and mitigate to the extent possible any negative effects that the incident may have had in a timely manner.

Creighton University and its workforce members will not intimidate or retaliate against any workforce member or individual that reports the incident.

# 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.

**Security Incident**
A breach that leads to the actual, potential, or appearance of a violation of the confidentiality, integrity, or availability of ePHI.

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

RESPONSIBILITIES

All individuals identified in the scope of this policy are responsible for compliance with any sanction that is applied to them under this policy

Information Security Officer is responsible for reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the workforce member

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](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.