HIPAA Policies

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 (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 that passwords created and used to access, transmit, receive, or store PHI are properly safeguarded. Proper safeguards include:

- Passwords used to access, transmit, receive, or store PHI must be of sufficient complexity to ensure that it is not easily guessable.
- All passwords must be changed at least every 90 days.
- User accounts that have system-level privileges should not be the same account used by administrators for every day activities.
- Systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.
- Passwords must never be revealed over the phone to ANYONE.
- Passwords must never be revealed in an e-mail message.
- Passwords must never be revealed on questionnaires or security forms.
- User accounts that have system-level privileges must have a unique password from all other accounts held by that user.
- Passwords must not be disclosed to other workforce members or individuals.
- Workforce members must not allow other workforce members or individuals to use their password.
- Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

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.
System-Level Privileges
An account that has powers within the computer system, which are significantly greater than those available to the majority of users. Such accounts will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

RESPONSIBILITIES

Administrators of systems that maintain PHI are responsible for ensuring that passwords set by workforce members meet a minimum level of complexity.

Individuals who access PHI are responsible for choosing passwords that adhere to the password procedures defined by the system administrator.

Information Security Officer is responsible for validating that all systems that collect, maintain, use or transmit ePHI adhere 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.

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.