

System Access Policy

Policy:

It is the policy of Kewaunee County to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems by all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization's information systems and are extended even after termination or other conclusion of access. These safeguards have been established to address the HIPAA Security regulations.

The policy is written from the perspective of a covered entity. The term "covered entity" may be replaced by the term "business associate" where appropriate within the policy when a business associate is performing those activities that are associated with the business associate's requirements under the HIPAA Privacy Rule and Security Rule.

Responsible for Implementation:

Security Officer & Privacy Officer.

Applicable To:

All workforce members and any other individual provided access.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Key Definitions:

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Minimum Necessary Information: Protected health information that is the minimum necessary to accomplish the intended purpose of the access, acquisition, use, disclosure, or request. The "minimum necessary" standard applies to all protected health information in any form.

Protected Health Information (PHI). Individually identifiable health information:

- That is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual
- The provision of health care to an individual
- The past, present, or future payment for the provision of health care to an individual
- Excluding:
 - Regarding a person who has been deceased for more than 50 years;
 - Employment records held by a covered entity in its role as employer; and
 - Education records covered by the Family Educational Rights and Privacy Act (FERPA).

Role: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

Workforce: Employees, volunteers, board members, community representatives, trainees, students, contractors, and other persons whose conduct, in the performance of work for the covered entity or business associate, is under the direct control of such covered entity, whether or not they are paid by covered entity or business associate.

Workstation: Any electronic computing device, such as a laptop or desktop computer, including virtual desktops, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.

Procedures

1. Access Establishment and Modification

- (a) All requests for access to any of the organization’s information systems applications must be approved by the requestor’s immediate supervisor.
 - 1. Training related to security, confidentiality, and incident reporting must occur before log in credentials are issued.

2. Workforce Clearance Procedures

- (a) The level of security assigned to a user to the organization’s information systems is based on the minimum necessary information access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
- (b) All access requests are treated on a ‘least-access principle’; blanket access is not provided for any user.
- (c) Any access not specifically authorized is prohibited.

3. Access Authorization

- (a) Role based access for each information system/application are pre-approved by each individual department. Any access must be based on the minimum necessary information needed for the user’s role.
- (b) Refer to the remote access policy for details relating to remote access.

4. Person or Entity Authentication

Each user has and uses a unique User Login ID and password that identifies him/her as the user of the information system.

5. Unique User Identification

- (a) Access to the organization's information systems/applications is controlled by requiring unique User Login ID's and passwords for each individual user.
- (b) Password requirements should be based on current industry and NIST standards whenever possible.
- (c) Passwords are not displayed at any time.
- (d) Users should not select passwords that may be easily guessed or obtained using personal information.
- (e) The IT Department assigns a User Login ID and generic password for each user to utilize for first time access into each information system.
- (f) Users must change their password upon first-time use of the information system.

6. Password Management

- (a) User Login IDs and passwords are used to control access to the organization's information systems and should not be disclosed. Under rare circumstances IT support may need a user ID and password. When that happens the password may be shared but should be changed to a new password as soon as possible.
- (b) Users may not allow anyone for any reason to have access to any information system using another user's unique User Login ID and password with the exception of IT support as outlined above.
- (c) Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database whenever possible.
- (d) Users that do not recall their password may contact the the IT Department.
- (e) Passwords are inactivated upon an employee's termination.
- (f) If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the IT Department.

7. Automatic Logoff

- (a) Users are required to make information systems inaccessible by any other individual when unattended by the users.
- (b) Users must log off information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.
- (c) Information systems should automatically log users off the systems after 5 minutes of inactivity.

8. Workstation Use

- (a) Workstations should only be used for authorized business purposes.
- (b) When possible workstations should be placed in secure areas. Workstations in patient rooms or public areas must be logged off or locked when not in use. Users must take actions to prevent unauthorized viewing.
- (c) All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.
- (d) Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.

9. Workstation Security

- (a) Workstations are the property of organization and must always remain on the premises, unless prior authorization has been granted for removal of workstations from the premises.
- (b) Workstations utilized off organization's premises are protected with security controls equivalent to those for on-site workstations.
- (c) Users may access and utilize workstations as assigned by their supervisor.
- (d) Supervisors are responsible for monitoring use of workstations.
- (e) All users must report unauthorized workstation use to the Security Officer or designee.
- (f) The organization must install on all workstations anti-virus software to prevent transmission of malicious software. This software is regularly updated.
- (g) Portable workstations are also subject to the same safeguards and protections. Portable workstations are maintained in a safe and secure manner when transported.
- (h) Networks are secured with a Firewall.
 - 1. Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
 - 2. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
 - 3. Mechanisms to log failed access attempts are in place.
 - 4. The configuration of firewalls used to protect networks is approved by the Technical Security Officer or designee and maintained by the IT Department.
 - 5. Firewalls need to be maintained as staff change positions.
- (i) Servers are located in a physically secure environment and are on a secure network with firewall protection.
 - 1. The system administrator or root account is password protected.
 - 2. A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
 - 3. All unused or unnecessary services are disabled.

10. Termination Procedures

- (a) The department heads, users, and their supervisors are required to notify the IT Department upon completion and/or termination of access needs.
- (b) The department heads, users, and supervisors are required to notify the IT Department to terminate a user's access rights if there is evidence or reason to believe the following:
 - 1. The user has been using their access rights inappropriately.
 - 2. A user's password has been compromised.
- (c) The IT Department will terminate users' access rights immediately upon notification.
- (d) The IT Department audits and may terminate access of users that have not logged into organization's information systems/applications for a period of over six (6) months.