Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #

Access Control Procedure

Last Revised: 3/15/2006	*Approved:*

Scope of Procedure

The scope of this Policy covers the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain EPHI to assure that such systems are accessed only by those persons or software programs that have been granted access rights under the HIPAA Security Policy #4 -- Information Access Management.

Procedure

1) Unique User Identification and Password

a) Purpose: To uniquely identify and track each user or workforce member for the purpose of monitoring access control to all RO-managed networks, systems, and applications that contain EPHI

b) Any user or workforce member that requires access to any network, system, or application that access, transmits, receives, or stores EPHI, must be provided with a unique user identification string. (See HIPAA Security Policy #3 -- Workforce Security and HIPAA Security Policy #4 -- Information Access Management).

c) When requesting access to any network, system, or application that accesses, transmits, receives, or stores EPHI, a user or Workforce member must supply his or her previously assigned unique user identification in conjunction with a secure password to gain access.

d) Each user's or Workforce member's password must meet the following conditions:

- Passwords must be a minimum of six or more characters in length. Administrative, system and other privileged accounts should employ a password of eight or more characters in length
- Passwords must incorporate three of the following characteristics:
  - Any lower case letters (a-z)
  - Any upper case letters (A-Z)
  - Any numbers (0-9)
  - Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)
- Passwords must not be words found in a Dictionary.
- Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.

- If a system does not support the minimum structure and complexity as detailed in the aforementioned guidelines, one of the following procedures must be implemented:
    - The password assigned must be adequately complex to insure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
    - The legacy system must be upgraded to support the requirements of this Paragraph d) as soon as administratively possible.
    - All EPHI must be removed and relocated to a system that supports the foregoing security password structure.
- Users or workforce members must not allow another user or workforce member to use their unique user identification or password.
- Users or workforce members must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner.

e) Each user and workforce member must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications. If a user or workforce members believes their user identification has been comprised, they must report that security incident to the appropriate Security Officer (See HIPAA Security Policy #6-- Incident Response and Reporting).

2) Emergency Access

a) WU HIPAA Security Policy requires procedures to ensure that access to a system that contains EPHI and is used to provide patient treatment is made available to any caregiver in the case of an emergency if the denial or strict access to that EPHI could inhibit or negatively affect patient care. During extreme emergency conditions, RO would rely upon BJH electronic access to the IMPAC electronic medical record as well as BJH Health Informations Management (HIM) for access to the physical medical record.

3) Automatic Logoff

a) Servers, workstations, or other computer systems containing EPHI repositories that have been classified as high risk (See HIPAA Security Policy #2 -- Security Management) must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity. WU RO manages no high risk data repositories.

b) Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (i.e., password protected screensaver that blacks out screen activity.) The aforementioned systems must block a user session after a maximum of 15 minutes of inactivity.

c) Applications and databases using medium or high risk EPHI, such as electronic medical records (EMR), must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity.

d) Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.

e) If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:

- The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.
- The system must be moved into a secure environment.
- All EPHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.

f) When leaving a server, workstation, or other computer system unattended, Workforce members must lock or activate the systems automatic logoff mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing EPHI.

4) Encryption and Decryption

Encryption of EPHI as an access control mechanism is not required unless the custodian of said EPHI deems the data to be highly critical or sensitive. Encryption of EPHI is required in some instances as a transmission control and integrity mechanism. (See HIPAA Security Procedure #17 -- Transmission Security and HIPAA Security Procedure #15 -- EPHI Integrity)

5) Firewall Use

a) Purpose: WU HIPAA Security policy requires that all networks housing EPHI repositories must be appropriately secured.

b) Networks containing EPHI-based systems and applications must implement perimeter security and access control with a firewall.

c) Firewalls must be configured to support the following minimum requirements:

- Limit network access to only authorized workforce members and entities.
- Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
- Console and other management ports must be appropriately secured or disabled.
- Implement mechanism to log failed access attempts.
- Must be located in a physically secure environment.

d) WU HIPAA Security policy requires that each Business Unit document its configuration of firewall(s) used to protect networks containing EPHI-based systems and applications. This documentation must include firewall rules and must be submitted to and approved by the HIPAA Security Office.

6) Remote Access

a) Purpose: To ensure that all networks that contain EPHI based systems and applications are appropriately secured.

b) Dialup connections directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.

c) Authentication and encryption mechanisms are required for all remote access sessions to networks containing EPHI via an ISP (Internet service provider). Mechanisms utilized or planned within RO include: VPN clients, authenticated SSL web sessions, secure shell and secured Citrix client access.

d) The following security measures must be implemented for any remote access connection into a secure network containing EPHI:

- Use of technology to bypass authorized remote access mechanisms (e.g. VPN) is strictly prohibited. For example, use of remote control software and applications such as PC Anywhere or GoToMyPC.com to bypass VPN or Citrix access mechanisms is not permitted.
- Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of session.
- Remote access workstations must employ a virus detection and protection mechanism. (See HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security)
- Users of remote workstations must comply with HIPAA Security Policy # 10 - Workstation Use)

e) VPN split-tunneling is not permitted for connections originating from outside the WU network (WUCON or .wustl.edu) or from an insecure network within the Washington University domain.

f) All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, 128-bit encryption.

g) WU HIPAA Security Policy requires that the Business Unit of any Workforce member requesting remote access to a secure network containing EPHI-based systems and applications must insure that the remote workstation or mobile device being used by said Workforce member initially meets (and continues to meet) the security measures detailed in HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security. The owner (managing entity) of the secure network must insure that the previous requirement has been satisfied before access is granted.

- Users who require remote access must work with OIS (Oncology Information Systems) to insure setup of all required security measures.
- OIS will employ inventory and remote patch distribution software to insure that client computers requesting remote access continue to comply with all required security measures.

7) Wireless Access

a) Purpose: To ensure that all networks that contain EPHI based systems and applications and that support wireless access are appropriately secured.

b) Wireless access to networks containing EPHI-based systems and applications is permitted in RO so long as the following security measures have been implemented:

- Encryption must be enabled. (See HIPAA Security Policy # 17 – Transmission Security)
- MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
- All console and other management interfaces must have been appropriately secured or disabled.
- Wireless access points are managed by the subnet network management group (OIS). (No unmanaged, ad-hoc, or rogue wireless access points are allowed).

c) Note: Not all wireless LANs utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit EPHI may not allow encryption of that data stream. It has been determined that this is low risk because this implementation of infrared is very short distance and low power.

d) All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

e) WU HIPAA Security Policy requires that the Business Unit of any Workforce member requesting access to a secure wireless network containing EPHI-based systems and applications must insure that the wireless device being used by said Workforce member initially meets (and continues to meet) the security measures detailed in HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security. The owner (managing entity) of the secure wireless network must ensure that the previous requirement has been satisfied before access is granted.

- Users who require remote access must work with OIS (Oncology Information Systems) to insure setup of all required security measures.
- OIS will employ inventory and remote patch distribution software to insure that client computers requesting remote access continue to comply with all required security measures.