Technical Safeguards

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR ACCESS CONTROLS

Category: HIPAA Security (Technical)	**Approved:**
Policy #:	**Effective:**
Version: 1.0	**Revised:**

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule and all applicable laws, regulations and organization policies and procedures. The organization has adopted this policy to ensure that access to electronic protected health information (ePHI) is only available to those persons or programs that have been appropriately granted such access.

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.

POLICIES AND PROCEDURES

UNIQUE USER IDENTIFICATION AND PASSWORD

1. 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.

2. 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.

3. Each user's or workforce member's password must meet the following:

    - Passwords must be a minimum of twelve characters in length.
    - Passwords must incorporate at least two alpha (letters) and two numeric (numbers) characters
    - 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:
        i. The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
        ii. The legacy system must be upgraded to support the requirements as soon as administratively possible.
        iii. 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.

4. 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 member believes their user identification has been comprised, they must report that security incident to the Security Officer or their immediate supervisor.

EMERGENCY ACCESS

1. Retrieve critical system and data backups from offsite location.

2. Retrieve hardware stored off-site.

3. Restore system and data to hardware.

4. Allow access only to those workforce members whose job function affects plan participant care.

5. ePHI repositories that do not affect individual care are not subject to the foregoing emergency access requirement.

AUTOMATIC LOGOFF

1. Servers, workstations, or other computer systems containing ePHI repositories must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.

2. 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 terminate a user session after a maximum of 15 minutes of inactivity.

3. Applications and databases using ePHI must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes of inactivity.

4. 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.

5. 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 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.

6. 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.

ENCRYPTION AND DECRYPTION OF EPHI MAINTAINED ON INTERNAL DATABASES

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 may be required in some instances as a transmission control and integrity mechanism.

FIREWALL USE

1. Networks containing ePHI-based systems and applications must implement perimeter security and access control with a firewall.

2. 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.

3. The organization must document its configuration of firewalls used to protect networks containing ePHI-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.

REMOTE ACCESS

1. 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.

2. Authentication and encryption mechanisms are required for all remote access sessions to networks containing ePHI via an ISP (internet service provider) or dialup connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.

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

   - Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications such as PC Anywhere or GoToMyPC.com are 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.
   - Users of remote workstations must comply with HIPAA Security Policy - Workstation Use.

4. VPN split-tunneling is not permitted for connections originating from outside the organization's network.

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

WIRELESS ACCESS

1. Wireless access to networks containing ePHI-based systems and applications is permitted so long as the following security measures have been implemented:

   - Encryption must be enabled. (See HIPAA Security Policy – 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 have been appropriately secured or disabled.

2. Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing ePHI-based systems and applications.

3. All wireless LANs do not 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.

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

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR AUDIT CONTROLS

Category: HIPAA Security (Technical)	**Approved:**
Policy #:	**Effective:**
Version: 1.0	**Revised:**

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule and all applicable laws, regulations and organization policies. The organization has adopted this policy to set forth the internal audit procedures for security of electronic protected health information (ePHI).

The scope of this policy covers the hardware, software and/or procedural mechanisms that will be implemented by the organization to record and examine activity in information systems that contain or use ePHI.

POLICIES AND PROCEDURES

AUDIT CONTROL MECHANISMS

1. The organization must utilize a mechanism to log and store system activity for each system that contains or accesses ePHI.

2. Each system's audit log **must** include, but is not limited to, user ID, login date/time, and activity time. Audit logs **may** include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.

3. System audit logs must be reviewed at least once every 180 days.

AUDIT CONTROL AND REVIEW PLAN

1. The audit logs must be reviewed at least once every 180 days.

2. Any potential threats or incidents must be reported to the Security Officer

3. The Security Officer must investigate all reports of threats or incidents.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR DATA INTEGRITY

Category: HIPAA Security (Technical)	**Approved:**
Policy #:	**Effective:**
Version: 1.0	**Revised:**

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule and all applicable laws, regulations and organization policies. The organization has adopted this policy to outline the procedures to be used to protect electronic protected health information (ePHI) from improper alteration and destruction.

The scope of this policy is to outline the appropriate data authentication measures that the organization must implement to ensure that ePHI is not improperly altered or destroyed. Data authentication is the process used to validate data integrity, verify that the data sent is the same data that is received and ensure the integrity of data stored and retrieved.

POLICIES AND PROCEDURES

TRANSMISSION INTEGRITY AND AUTHENTICATION

The organization will implement SSL and data checksum technology for all high-risk ePHI that is transmitted outside the organization's network, to corroborate that the ePHI has not been altered or destroyed during transmission.

SYSTEM INTEGRITY

The organization must implement a mechanism for all systems containing high-risk ePHI to ensure that ePHI has not been altered or destroyed by a virus or other malicious code to include:

1. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

2. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.

DATA AT REST INTEGRITY

The organization must use error-correcting memory and storage to authenticate data that is being stored and retrieved. For high-risk ePHI, a DES (Digital Encryption Standard) encryption mechanism or data checksum may be used to ensure the integrity of data at rest. The use of data authentication mechanisms other than virus detection is not required for low-risk ePHI.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR
PERSON AND ENTITY AUTHENTICATION

Category: HIPAA Security (Technical)	**Approved:**
Policy #:	**Effective:**
Version: 1.0	**Revised:**

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule and all applicable laws, regulations and organization policies. The organization has adopted this policy to set forth the authentication requirements for access to the organization's electronic protected health information (ePHI).

The scope of this policy covers the procedures to be implemented by the organization to verify that a person or entity seeking access to ePHI is the person or entity claimed.

POLICIES AND PROCEDURES

1. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.

2. Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's user ID and password, smart card, or other authentication information.

3. Workforce members are not permitted to allow other persons or entities to use their unique user ID and password, smart card, or other authentication information.

4. A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting ePHI.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR TRANSMISSION SECURITY

Category: HIPAA Security (Technical)	**Approved:**
Policy #:	**Effective:**
Version: 1.0	**Revised:**

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule and all applicable laws, regulations and organization policies. The organization has adopted this policy to outline the requirements for transmission of organization electronic protected health information (ePHI) to ensure the security and integrity of such ePHI.

The scope of this policy covers the technical security measures that the organization will implement to guard against unauthorized access to or modification of ePHI that is being transmitted over an electronic communications network or via any form of removable media.

POLICIES AND PROCEDURES

EPHI TRANSMISSIONS TO NON-ORGANIZATIONS OR PLAN SPONSOR (FOR EMPLOYER GROUP HEALTH PLANS)

To appropriately guard against unauthorized access to or modification of ePHI that is being transmitted from the organization's an outside network, the following procedures outlined must be implemented.

1. All transmissions of ePHI from the organization's network to an outside network must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said ePHI must be encrypted before transmission.

2. Prior to transmitting ePHI from the organization's network to an outside network the receiving person or entity must be authenticated. (see HIPAA Security Policy - Person or Identity Authentication)

3. All transmissions of ePHI from the organization's network to an outside network should include only the minimum amount of ePHI.

EPHI TRANSMISSIONS USING ELECTRONIC REMOVABLE MEDIA

1. When transmitting ePHI via removable media, including but not limited to, floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must:

   - Use an encryption mechanism to protect against unauthorized access or modification.
   - Authenticate the person or entity requesting said ePHI in accordance with HIPAA Security Policy - Person or Entity Authentication.
   - Send the minimum amount of said ePHI required by the receiving person or entity.

2. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

EPHI TRANSMISSIONS USING EMAIL OR MESSAGING SYSTEMS

1. The transmission of ePHI from the organization to a **<patient/individual/plan participant>** via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- The <**patient/individual/plan participant**> has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.
- The <**patient/individual/plan participant**> has formally authorized the organization to utilize an email or messaging system to transmit ePHI to them.
- The <**patient/individual/plan participant**>'s identity has been authenticated.
- The email or message contains no excessive history or attachments.

2. The transmission of ePHI from the organization to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

    - The receiving entity has been authenticated.
    - The receiving entity is aware of the transmission and is ready to receive said transmission.
    - The sender and receiver are able to implement a compatible encryption mechanism.
    - All attachments containing ePHI are encrypted.

3. The transmission of ePHI within the organization via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of ePHI is being transmitted and the ePHI is not high risk, sensitive or critical. ePHI that is high risk, sensitive or critical should not be sent through clear text email; such ePHI should be sent via encrypted attachment or other secure measure. If an email or message includes an attachment that contains ePHI, the attachment must be encrypted or password protected before transmission.

4. Email accounts that are used to send or receive ePHI must not be forwarded to non-organization accounts.

EPHI TRANSMISSIONS USING WIRELESS LANS AND DEVICES

1. The transmission of ePHI over a wireless network within the organization's network is permitted if the following conditions are met:

    - The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
    - The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

2. If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.