Physical Safeguards

WAUPACA COUNTY
FACILITY REPAIR DOCUMENTATION FORM

Item Repaired	Date of Repair	Time of Repair	Type of Repair	Person Who Performed Repair

WAUPACA COUNTY
HARDWARE AND ELECTRONIC MEDIA TRACKING FORM

Equipment	Model	Serial Number	Asset Tag	Warranty Date	User Name	User Location

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR DEVICE AND MEDIA CONTROLS

Category: HIPAA Security (Physical)	**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 ensure that the receipt and removal of hardware and electronic media containing electronic protected health information (ePHI) complies with the Security Regulations.

The scope of this policy is to outline the policy and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of such items within the facility.

POLICIES AND PROCEDURES

DESTRUCTION OF WORKSTATIONS, STORAGE DEVICES OR REMOVABLE MEDIA

1. Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device or media does not contain ePHI.

2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.

3. If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal (such as reformatting the hard drive of a workstation).

REUSE OF WORKSTATIONS, STORAGE DEVICES OR REMOVABLE MEDIA

1. Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain ePHI.

2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.

3. If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse (such as reformatting the hard drive of a workstation).

4. 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, the use of a data destruction tool between uses is not necessary.

MOVEMENT OF WORKSTATIONS AND EQUIPMENT HOUSING EPHI

1. If the device or media contains the only copy of ePHI that is required or needed, an exact retrievable copy of ePHI is required prior to the movement of equipment storing such ePHI.

2. When using storage devices and removable media to transport ePHI, the organization must track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR FACILITY ACCESS CONTROLS

Category: HIPAA Security (Physical)	**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 ensure that physical access to ePHI is appropriately limited.

The scope of this policy covers the procedures that will limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

POLICIES AND PROCEDURES

FACILITY SECURITY PLAN

To safeguard all facilities, systems, and equipment used to store electronic protected health information (ePHI) against unauthorized physical access, tampering, or theft; the organization will implement the following:

1. Contingency Operations – allow physical facility access during emergencies to support restoration of data under the Disaster Recovery Plan.

    a. A list containing the names and job titles that will have access to facilities during emergencies will be maintained by the Security Officer.
    b. During emergencies only workforce members and business associates whose names appear on the list will be granted access to systems containing ePHI.

2. Access Control and Validation – Control and validate workforce members' access to facilities based on their role or function.

    a. The Security Officer in conjunction with department supervisors will develop a list based on job function to determine who should have what level of access to systems containing ePHI.
    b. This list will reside with the Security Officer and the department supervisors.
    c. When a workforce member joins a department their physical access to ePHI will be granted based on their job function, as detailed on the access list.
    d. When a workforce member leaves a department all access rights for that workforce member will be revoked.

3. Physical Access Records – log physical access to any facility containing ePHI-based systems. Examples of facilities requiring physical access records are computer and system rooms.

    a. A log to track who entered facilities that house ePHI based systems will be maintained at each facility. The log will track the workforce member's name, identification number (if any) and the time and date they entered the facility.

4. Maintenance Records – document maintenance, repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

    a. The log to document repairs to physical security components will be maintained by the Physical Plant Operations Manager (or equivalent) and the Security Officer.
    b. The log will document the date and time of the repair, type of repair, and, who performed the repair.

WORKFORCE ACCESS CONTROLS

1. The organization must control and validate workforce member access to all facilities used to house ePHI based systems.

    a. Before entering facilities used to house ePHI based systems employees must sign into the access log or show proper organization or plan sponsor issued, identification.

2. If the organization or plan sponsor utilizes employee identification badges the workforce members must wear their identification badges at all times while in facilities that contain systems that house ePHI.

3. Each facility must adopt appropriate access control mechanisms to control physical access to all facilities containing ePHI-based systems. Code locks, badge readers, and key locks are examples of physical access control mechanisms.

VISITOR ACCESS CONTROLS

1. The organization and plan sponsor will control, validate, and document visitor access to any facility used to house ePHI based systems. Visitors include vendors, repair personnel, and other non-workforce members.

2. All visitors who require access to facilities containing ePHI based systems must sign in and provide information regarding their identity and the purpose of their visit.

3. All visitors must be provided a temporary identification badge or be escorted to and from their destination.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR WORKSTATION SECURITY

Category: HIPAA Security (Physical)	**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 physical safeguards that will apply to hardware that may be used to access, transmit, store or receive electronic protected health information (ePHI).

The scope of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained and that access is restricted to authorized users. Each workstation that is used to access, transmit, receive or store ePHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The server, desktop computer system, or wireless computer system must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The workstation must not be used to send, receive or store ePHI.

POLICIES AND PROCEDURES

SERVER SECURITY REQUIREMENTS

1. All servers used to access, transmit, receive or store ePHI must be located in a physically secure environment.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system.

4. 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.

5. Servers must be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity.

6. All unused or unnecessary services shall be disabled.

DESKTOP SYSTEM SECURITY REQUIREMENTS

1. Each desktop system used to access, transmit, receive or store ePHI must be located in a physically secure environment.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system.

4. 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.

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

6. All unused or unnecessary services must be disabled.

7. Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:

    - An inactivity timer or automatic logoff mechanisms must be implemented.
    - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.

MOBILE SYSTEMS SECURITY POLICY

1. All mobile systems used by workforce members to access, transmit, receive or store ePHI must be appropriately secured.

2. The system administrator or root account must be password protected.

3. A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.

4. 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.

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

6. All unused or unnecessary services must be disabled.

7. Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:

    - A theft deterrent device (such as a laptop locking cable) must be utilized when the device is unattended.
    - An inactivity timer or automatic logoff mechanism must be implemented.
    - Reasonable safeguards must be in place to prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.

8. Personal Digital Assistants (PDAs) and other handheld mobile devices must not be used for long-term storage of ePHI. ePHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device, with a storage time not to exceed 30 days.

9. Each mobile system that is used to access, transmit, receive, or store ePHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR WORKSTATION USE

Category: HIPAA Security (Physical)	**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 physical measures required to protect electronic information systems and related equipment from unauthorized use.

The scope of this policy is to specify the proper functions to be performed, the manner in which such functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information (ePHI).

POLICIES AND PROCEDURES

PASSWORDS

1. All systems will require a valid user ID and password.

2. Passwords will have the following characteristics:

    a. Passwords will be at least twelve characters long
    b. All user-chosen passwords should have at least two alpha (letter) and two numeric (number) characters
    c. The use of control characters and non-printing characters is prohibited

3. It is recommended that all users change their passwords at least every six months.

4. In the event of a suspected or actual password breach those passwords are to be changed immediately.

5. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator.

6. The display or printing of passwords will be masked so that unauthorized parties will not be able to observe or recover them.

7. Passwords will not be stored in written or readable form.

8. Upon termination all passwords for the employee will be immediately changed or deactivated.

ACCESS

1. Computer screens will be positioned in such a manner that only authorized users may see the information contained on the screen.

2. A notice, at system start-up, warning that only those with proper authority should access the system will be displayed initially before signing onto the system or a written notice with a warning that only those with proper authority should access the system will be displayed near the computer terminal.

3. Individuals who are not employees, contractors, consultants, or business partners will not be granted access to any systems.

4. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.

5. Employees will logoff the system before going to lunch or taking breaks.

6. Employees will logoff the system before they end their shift for the day.

7. The room where the workstation is contained will be locked when not in use.

8. All removable media (e.g. CD-ROMs. backup tapes, diskettes, and etc.) containing protected health information will be stored in a locked cabinet to prevent unauthorized use.

9. All removable media (e.g. CD-ROMs backup tapes, diskettes, etc.) containing protected health information that will no longer be used will be reformatted or destroyed preventing any protected health information from being seen by unauthorized individuals.

10. Printed versions (hardcopy) of protected health information will be shredded before it is discarded.

11. System access will be reviewed annually to remove identification codes and passwords of users who no longer require access.

REMOTE ACCESS

1. Remote access via modem should be through an approved security mechanism such as a dial back system, or only allowing modem connectivity from specified phone numbers.

2. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator.

INTERNET

1. Use of the Internet via our network will be primarily for business or professional development.

2. Use of the Internet via our network is not permitted for personal use.

3. A firewall will be installed to protect against unauthorized intrusion.

E-MAIL (ELECTRONIC MAIL)

1. Prohibited use of the electronic mail system includes, but is not limited to:

    a. Disclosure of a **<patient/individual/plan participant>** personal health information without appropriate authorization
    b. Transmission of information inside or outside of the organization without a legitimate business need for the information
    c. Use for marketing purposes without explicit permission of the plan participant

2. The following types of transactions (prescription refill, appointment scheduling, etc.) and sensitive subject matter (HIV, mental health, etc.) should not be sent over e-mail.

3. <**Patients/Individuals/Plan participants**> will be instructed to put category of transaction in subject line of message for filtering: "claims question", "eligibility", "enrollment", "billing question".

4. **<Patients/Individuals/Plan participants>** will be instructed to put their name and **<patient/individual/plan participant>** identification number in the body of the message.

5. All messages will be printed, with replies and confirmation of receipt, and placed in **<patient/individual/plan participant>**'s record.

6. We will send a new message to inform the **<patient/individual/plan participant>** of completion of request.

7. The sharing of organization e-mail accounts with family members is strictly prohibited.

8. We will double-check all "To:" fields prior to sending messages.

9. We will perform at least weekly backups of mail onto long-term storage.

10. The use of distribution lists for distributing confidential information is strictly prohibited.

11. The subject line will contain a notation referring to the confidential or sensitive nature of the information.

12. **<Patients/Individuals/Plan participants>**'s authorization should be obtained before forwarding protected health information to an external third party not bound by a Business Associate Agreement with the organization.

13. **<Patients/Individuals/Plan participants>**'s e-mail addresses will not be supplied to third parties for advertising or any other use.

14. When an e-mail account will not be monitored during a vacation or office closure, an auto reply should be sent notifying the sender that the intended recipient is away.

15. Upon termination of employment the e-mail account will be deactivated.

MONITORING OF WORKSTATION USE

Workforce members that use the organization's information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, the organization may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.

REMOVAL OF WORKFORCE MEMBERS PRIVILEGES

The organization may remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

REPORTING COMPLAINTS

Complaints or concerns about another's use of the organization's computer resources should be directed to the Security Officer or your immediate supervisor.

WAUPACA COUNTY
WORKSTATION REASSIGNMENT FORM

Equipment	Model	Serial Number	Asset Tag	Reassignment Date	Previous User	New User