Administrative Safeguards

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR EVALUATION

Category: HIPAA Security (Administrative)	**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 its security policies and procedures are up to date and effective in ensuring the confidentiality, integrity and availability of electronic protected health information (ePHI) created, received, maintained and transmitted by the organization

The scope of this policy covers the procedures that will ensure that each security policy and procedure adopted by the organization is periodically evaluated for technical and non-technical viability.

POLICIES AND PROCEDURES

INITIAL EVALUATION

The organization's security policies and procedures initially should be evaluated to determine their compliance with the HIPAA Security Regulations. Once compliance with the HIPAA Security Regulations is established, the organization's security policies and procedures should be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of ePHI.

PERIODIC EVALUATION BY HIPAA SECURITY OFFICER

1. The HIPAA Security Officer will review on an on-going basis the viability of the organization's security policies and procedures.

2. The HIPAA Security Officer will develop and implement any necessary security policy or procedure changes.

EVALUATION UPON OCCURRENCE OF CERTAIN EVENTS

In the event that one or more of the following events occur, the policy and procedure evaluation process will be immediately triggered:

- Changes in the HIPAA Security Regulations or Privacy Regulations
- New federal, state, or local laws or regulations affecting the privacy or security of protected health information (PHI)
- Changes in technology, environmental processes or business processes that may affect HIPAA security policies or procedures
- A serious security violation, breach, or other security incident occurs

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
RISK MANAGEMENT

Waupaca County has identified the following risks and deficiencies while going through the HIPAA Security Documentation Kit's policies and procedures. The goal is to fix these as quickly as possible to reduce risks and vulnerabilities to a reasonable and appropriate level and to ensure compliance with the HIPAA Security regulations.

Safeguard	Implementation Standard	Implementation Specification	Document	Document Page/Line	Action Item	Priority	Assigned To	Date to Be Completed	Date Completed

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR
SECURITY AWARENESS AND TRAINING

Category: HIPAA Security (Administrative)	**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 a framework for a security awareness and training program for all members of its workforce.

The scope of this policy covers the components of the security awareness and training program. The program will include:

- Security reminders
- Procedures for guarding against, detecting and reporting malicious software
- Procedures for monitoring log-in attempts and reporting discrepancies
- Procedures for creating, changing and safeguarding passwords

POLICY AND PROCEDURES

SECURITY REMINDERS

1. The organization will issue security updates to the workforce when changes to the HIPAA Security Rule or the organization's HIPAA Security policies and procedures occur.

2. The organization will issue warnings to the workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents.

3. The organization will issue security reminders to the workforce at least once every 180 days.

PROTECTION FROM MALICIOUS SOFTWARE

The organization will implement hardware and software to guard against, detect and report to the appropriate persons new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

1. The organization will train its workforce to identify and protect against malicious code and software.

2. Workforce members must notify the HIPAA Security Officer if a virus, worm or other malicious code has been identified and is a potential threat to other systems or networks.

3. The Security Officer is responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

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

© Copyright 2002-2017, HIPAATraining.com

LOG-IN MONITORING

1. The organization must implement software to log and document failed login attempts on each system containing ePHI.

2. The organization must review such login activity reports and logs on a periodic basis. The interval of the login activity review must not exceed, but may be less than, 180 days.

3. All failed login attempts of a suspicious nature, such as continuous attempts, must be reported immediately to the HIPAA Security Officer.

PASSWORD MANAGEMENT

To ensure that passwords created and used by the organization's workforce to access any network, system, or application used to access, transmit, receive, or store ePHI are properly safeguarded and to ensure that the workforce is made aware of all password related policies, the following minimum procedures must be followed:

1. All workforce members that access networks, systems, or applications used to access, transmit, receive, or store ePHI must be supplied with a unique user identification and password to access the aforementioned ePHI.

2. All workforce members must supply a password in conjunction with their unique user identification to gain access to any application or database system used to create, transmit, receive, or store ePHI.

3. A generic user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to ePHI. An additional unique user identification and password must be supplied to access applications and database systems containing ePHI.

4. All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store ePHI must be of sufficient complexity to ensure that it is not easily guessable.

5. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI, must ensure that passwords set by workforce members meet the minimum level of complexity.

6. Managers of networks, systems, or applications used to access, transmit, receive, or store ePHI are responsible for making workforce members aware of all password-related policies and procedures, and any changes to those policies and procedures.

7. Password aging times may be implemented in a manner commensurate with the criticality and sensitivity of the ePHI contained within each network, system, application or database, but are not required.

8. Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

    - Passwords are only to be used for legitimate access to networks, systems, or applications.
    - 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.

© Copyright 2002-2017, HIPAATraining.com

SECURITY TRAINING PROGRAM

1. The organization is responsible for ensuring that its workforce, and those members of the plan sponsor's workforce that have access to ePHI, have the appropriate level of HIPAA Security training so that all workforce members who access, receive, transmit or otherwise use ePHI or who set up, manage or maintain systems and workstations that access, receive, transmit, or store ePHI are familiar with the organization's HIPAA Security policies and procedures and their responsibilities regarding such policies and procedures. Appropriate training must consist of, but is not limited to, the following requirements:

    - HIPAA Security Policies
    - HIPAA Business Associate Policy
    - HIPAA Sanction Policy
    - Confidentiality, Integrity and Availability
    - Individual Security Responsibilities
    - Common Security Threats and Vulnerabilities

2. The organization is responsible for ensuring that all information technology staff members and all workforce members who are responsible for the setup, installation or management of computer systems and networks containing ePHI have the appropriate level of HIPAA Security training. HIPAA Security training for these workforce members must consist of, but is not limited to, the following requirements:

    - HIPAA Security Policies
    - HIPAA Business Associate Policy
    - HIPAA Sanction Policy
    - Confidentiality, Integrity and Availability
    - Individual Security Responsibilities
    - Common Security Threats and Vulnerabilities
    - Password Structure and Management Procedures
    - Server, desktop computer, and mobile computer system security procedures, including security patch and update procedures and virus and malicious code procedures
    - Device and media control procedures
    - Incident response and reporting procedures

3. The organization must ensure that the appropriate information technology staff members are aware of and trained to comply with the following HIPAA Security plans and procedures:

    - Log-in monitoring procedures
    - Audit Control and Review Plan
    - Data Backup Plan
    - Disaster Recovery Plan

4. The organization must maintain formal documentation of the current level of HIPAA training for each of its workforce members.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
Confidentiality / Security Agreement

I have received Health Insurance Portability and Accountability Act (HIPAA) training and as such, I understand that while performing my official duties I may have access to protected health information. Protected Health Information (PHI) means individually identifiable health information that is transmitted or maintained in any form or medium. Protected health information is ***NOT*** open to the public. Special precautions are necessary to protect this type of information from unauthorized access, use, modification, disclosure, or destruction.

I agree to protect the following types of information:

All data elements described as protected health information (PHI) including but not limited to:

- Addresses
- Telephone numbers
- Fax numbers
- Electronic Mail addresses
- Social security numbers
- Medical record numbers
- Birth date
- Date of death
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial number, including license plate numbers
- Device identifiers and serial numbers
- Full face photographic images and any comparable images
- Client information (such as, disability insurance claimants, recipients of public social services, participants of state/federal programs, employers, etc.)
- Information about how automated systems are accessed and operate
- Any other proprietary information.
- Any other unique identifying number characteristic, or code

I agree to protect PHI by:

All of the following means including but not limited to:

- Accessing, using, or modifying confidential, sensitive, or PHI only for the purpose of performing my official duties
- Never attempting to access information by using a user identification code or password other than my own
- Never sharing passwords with anyone or storing passwords in a location accessible to unauthorized persons.
- Never exhibiting or divulging the contents of any record or report except to fulfill a work assignment.
- Never showing, discussing, or disclosing confidential, sensitive information, or PHI to or with anyone who does not have the legal authority or the "need to know"
- Storing confidential, sensitive information in a place physically secure from access by unauthorized persons.
- Never removing confidential, sensitive, or PHI from the work area without authorization.
- Disposing confidential, sensitive, or PHI by utilizing an approved method of destruction, which includes shredding, burning, or certified or witnessed destruction. Never disposing such information in the wastebaskets or recycle bins.
- Reporting any violation of confidentiality, privacy or security policies

© Copyright 2002-2017, HIPAATraining.com

Penalties

Unauthorized access, use, modification, disclosure, or destruction is strictly prohibited. The penalties for unauthorized access, use, modification, disclosure, or destruction may include disciplinary action up to and including termination of employment and/or criminal or civil action.

Waupaca County reserves the right to monitor and record all network activity including e-mail, with or without notice, and therefore users should have no expectations of privacy in the use of these resources.

Disclaimers

Nothing in this document creates any express or implied contractual rights. All employees are employed on an at-will basis. Employees have the right to terminate their employment at any time, and Waupaca County retains a similar right.

I certify that I have read, understood, and accept the Confidentiality Agreement above.

Full Name	**Department**
Signature	**Date**

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR CONTINGENCY PLANNING

Category: HIPAA Security (Administrative)	**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 its response to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI) complies with the HIPAA Security Regulations.

The scope of this policy covers the procedures that must be implemented in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Planning
- Emergency mode operation plan

POLICIES AND PROCEDURES

APPLICATIONS AND DATA CRITICALITY ANALYSIS

1. The relative criticality of specific applications and data must be assessed for purposes of developing a Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan.

2. The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

DATA BACKUP PLAN

1. The organization must create and maintain retrievable exact copies of all ePHI.

2. All files, records, images, voice or video files that may contain ePHI, must be backed up.

3. All media used for backing up ePHI must be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

4. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.

5. Data backup procedures must be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available.

© Copyright 2002-2017, HIPAATraining.com

DISASTER RECOVERY PLAN

1. The organization must restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner, to ensure that the organization can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI.

2. The organization must restore ePHI from data backups in the case of a disaster causing data loss, as follows:

    a. Retrieve critical system and data backups from offsite location.
    b. Retrieve hardware stored offsite.
    c. Restore system data and critical application data to hardware.

3. The organization will log system outages, failures, and data loss to critical systems.

4. The disaster recovery procedures outlined above must be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.

EMERGENCY MODE OPERATION PLAN

1. The organization must establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
CONTINGENCY PLAN
(164.308a7i)

CONTINGENCY PLAN SYSTEMS AND SERVICE LEVELS

Waupaca County depends on the following systems listed in the table below. Beside each system, there is a service level to respond to outages and disasters for that system. There are two types of service levels represented by the two columns in the table below:

Emergency Mode: To be able to respond and function at the most minimal level

Full Operation: To be able to respond at a level matching previous full operation

The rest of this document contains the detail of how that service level will be achieved for each system.

System	Emergency Mode	Full Operation
Telephone	24 hours	2 weeks
Email	24 hours	2 weeks
File Server	1 week	2 weeks
Domain Server	2 weeks	2 weeks
EMR	3 days	3 days
Billing System	1 week	1 week
CRM System	1 week	1 week
Desktops	3 days	4 weeks
Internet	3 days	4 weeks

WAUPACA COUNTY
EMERGENCY MODE OPERATION FOR TELEPHONE

In the case of emergency or disaster, in order to be able to respond and function at a minimal level for this system:

1) Our main telephone number is 715-258-6200

2) We will designate an individual or individuals to be able to handle calls and respond to incoming calls to our main number: Jesse Cuff

3) We will forward the main phone system telephone number to another phone such as a cell phone or other phone that is functional: Cell Phone

4) In order to forward that main telephone number, we will call Windstream/EarthLink at 920-965-7532 and have them assist us with transferring our Main Waupaca County Phone number to cell phone until or Location and system are useable.

WAUPACA COUNTY
FULL OPERATION FOR TELEPHONE

To be able to be fully operational again after an emergency or disaster:

1) We can call our telephone vendor WindStream/EarthLink at 920-965-7532 to request a repair or reinstallation.

2) The EarthLink's normal response time on repairs is 2-3 business days with another 2-3 days potentially for parts if they are not on hand. For reinstallations the lead time is 2 weeks.
   Corporate Network Solutions (listed below) - Shoretel equipment is on a similar schedule.

3) Our phone system make and model is ShoreTel and consists of the following modules:
   a. Voicemail
   b. Auto Attendant
   c. Caller ID
   d. Hunt Groups
   e. Work Groups

4) Alternative vendors
   a. Camera Corner Connecting Point (Installed our system but no longer our partner)

WAUPACA COUNTY
FULL OPERATION FOR DESKTOPS

To be able to be fully operational again after an emergency or disaster:

1) Our standard spec for PCs is:
    a. Corporate Network Solutions
    b. 8-16GB RAM
    c. 500GB – 1TB Hard Disk
    d. Intel i5 or above processor
    e. Windows 7 Pro 64 Bit or Windows 10 Pro 64 bit (Not home editions)
    f. 24" monitor (1900 x 1080)

2) We currently have 1 desktop or laptop per employee (not the case for Corrections or Patrol).

3) Vendors who we have purchased current desktops from:
    a. Corporate Network Solutions
    b. CDWG
    c. SHI

4) Alternative Vendors
    a. Heartland Business Systems

Disaster Recovery Plan (164.308a7iiB) (164.308a7iiC)

1) In case of damage to EPHI physical environment (Waupaca County Courthouse NOC)
    a. Backup data and limited hardware is available at the DR site (Highway, SO Annex, or Symco Tower)
    b. There is limited hardware in case of a DR event, and most likely equipment will need to be ordered
    c. Waupaca County will work with various vendors on hardware and software restoration.
        i. For the Information Technology Department – VEEAM backup system
    d. Waupaca County will work with Network Engineering(s) from Corporate Network Solutions for data recovery and hardware replacement.
    e. Waupaca County will let IT know which systems are most Critical, and those will be the systems that we will restore in order of importance
2) VEEAM Backup System is currently housed at the Waupaca County Highway Office – Veeam will eventually move to the Symco tower site once Fiber Optic cable is installed.
    a. AS400 CBU is housed at the SO Annex
        i. Backup tapes are taken home nightly by one of the IT Staff
3) All available IT staff will be working to restore either hardware or software, and the IT department will work with various contractors, vendors and engineers.
4) Waupaca County will work with those vendors who sign a business associate agreement either in advance or prior to working with Waupaca County ePHI in an emergency

Waupaca County does not have a full disaster plan for where employees will be working in case of events. Waupaca County IT can pick up the Veeam equipment and move it anywhere necessary while we wait for equipment orders from vendors.

WAUPACA COUNTY
EMERGENCY MODE AND FULL OPERATION
FOR EMR (ELECTRONIC MEDICAL RECORD) SYSTEM

The EMR system is a hosted based system provided by TCM. To be able to be fully operational again after an emergency or disaster:

1) Vendor contact information is:
    a. TCM
    b. David Ferri
    c. 320 Earls Ct. Deerfield, WI 60015
    d. (847) 948-9600
    e. David.ferri@clinicaldata.org

2) We are dependent on the vendor to be able to handle disaster recovery for this system. The vendor was contacted and has a disaster recovery plan in place. The following was the conversation about the details of their disaster recovery plan:

    a. Time for them to restore at current datacenter is 2 days
    b. Time for them to restore at an office data center is 3 days

Corporate Network Solutions, Inc.
Brian Van Asten
1624 E. Wisconsin Ave.
Appleton, WI 54911
REGULAR BUSINESS HOURS - (920) 832-8406
AFTER HOURS SUPPORT – (920) 427-7662
BRIAN.VANASTEN@CNSIWI.COM
HTTP://WWW.CNSIWI.COM/
PRIMARY SERVICES – NETWORK SUPPORT, SWITCHES, SERVERS, FIREWALLS, SANS, NASS, SHORETEL VOIP, BARRACUDA, DR, LAN, WAN, AFTER HOURS SUPPORT.

Multimedia Communications &Engineering
Joel Mikulsky
1624 E. Wisconsin Ave.
Appleton, WI 54911
OFFICE - (877) 870-6968 X701
CELLULAR – (920) 676-0494
JMIKULSKY@MCEWI.COM
HTTP://WWW.MCAE.BIZ/
PRIMARY SERVICES – FIBER OPTIC CABLE CONSULTATION AND INSTALL, REMOTE SITE CONNECTIVITY, CABLING, IT CONSULTATION, WIRELESS, RFP/RFB PREPARATION.

Faith Technologies.
James (Jay) Weber
2662 American Drive
PO Box 627
Appleton, WI 54912-0627
REGULAR BUSINESS HOURS - (920) 738-1500
REGULAR BUSINESS HOURS - (800) 274-2345
AFTER HOURS SUPPORT – (920) 841-0384
JAMES.WEBER@FAITHTECHNOLOGIES.COM
HTTPS://WWW.FAITHTECHNOLOGIES.COM/
PRIMARY SERVICES – NETWORK CABLING, LAN CONSULTATION, FIBERCONSULTATION

WISCNET.
Kika Barr (Senior Director of Operations and Service Success)
REGULAR BUSINESS HOURS - (608) 210-3955
KIKA.BARR@WISCNET.NET
HTTPS://WWW.WISCNET.NET/
INTERNET SERVICE PROVIDER

SUPPORT INFO BELOW IN RED TEXT

WISCNET TECHNICAL SUPPORT
support@wiscnet.net
608-442-6761 ext. 2
support@wiscnet.net

WISCNET NETWORK OPERATIONS CENTER
608-442-6761 ext. 1
24x7x365 telephone support

WISCNET BILLING SUPPORT
billing@wiscnet.net
608-442-6761 ext. 4
billing@wiscnet.net

WISCNET WORLD HEADQUARTERS
605 Science Drive
Madison, Wisconsin 53711
Phone: 608-442-6761
Fax: 608-210-3979

Revize
Joe Nagrant
1890 Crooks Rd
Troy, MI 48084
(248)-269-9263
joseph.nagrant@revize.com
www.revize.com
Primary service provided - website support/website host

Vanguard Systems, Inc.

Michael DiBattista
2901 Dutton Mill Road
Suite 220
Aston, PA 19014
(610)-891-7703
helpdesk@vansystems.com
www.vansystems.com
Primary service provided –Support for IMS21 scanning software

TCM.
David Ferri
320 Earls Ct.
Deerfield, WI 60015
(847) 948-9600
DAVID.FERRI@CLINICALDATA.ORG
HTTPS://WWW.CLINICALDATA.ORG/
PRIMARY SERVICES – DHHS – MEDICAL DATABASE – REPLACED DRI

Spillman / Motorola
Shaun Cavanaugh
4625 Lake Park Blvd.
Salt Lake City, UT 84120
(801) 902-1729
SHAUN.CAVANAUGH@MOTOROLASOLUTIONS.COM
HTTPS://WWW.SPILLMAN.COM/
PRIMARY SERVICES – SHERIFF DEPARTMENT DATABASE, MOTOROLA CALLWORKS

AT&T
Eric Watkins
8401 N Greenway Blvd
Middleton, WI 53562
(866) 484-4507
EW4720@ATT.COM
HTTPS://WWW.ATT.COM/
PRIMARY SERVICES – SO DISPATCH PHONE LINES, 10MB INTERNET

Heartland Business Systems (HBS)
Kurt Krueger
1700 Stephen St.
Little Chute, WI 54140
(800) 236-7914
TEAMKURT@HBS.COM
HTTPS://WWW.HBS.NET/
PRIMARY SERVICES – COMPUTER EQUIPMENT, SOFTWARE SUPPORT,PROOFPOINT SPAM FILTER

Mary Ledvina

N4029 Gasche Rd.
Luxemburg, WI 54217
(920) 845-5478
MARYLEDVINA@AOL.COM
PRIMARY SERVICES – PROGRAMMING SUPPORT FOR ISERIES/AS400 SOFTWARE

Tyler Technologies
Managed Services Customer
840 W. Long Lake Rd
Troy, MI 48098
(877) 734-3315
NWERP@TYLERTECH.COM
HTTPS://WWW.TYLERTECH.COM/CLIENT-SUPPORT/NEW-WORLD-ERP-SUPPORT
PRIMARY SERVICES – FINANCIAL AND HUMAN RESOURCE RECORD KEEPING

CDWG
Adam Flynn
CDW Plaza
120 S. Riverside
Chicago, IL 60606
(866) 723-3621
ADAMFLY@CDWG.COM
HTTPS://WWW.CDWG.COM/
PRIMARY SERVICES – EQUIPMENT, SOFTWARE PURCHASING AND SUPPORT, AS400 WARRANTY

iTechnology Services, LLC
Chuck Pulyeart (RETIRED in 2018)
2221 Cathedral Forest Dr.
Suamico, WI 54313
(920) 362-7155
CPUTLEART@ITECHSERVLLC.COM
PRIMARY SERVICES – INSTALLATION SUPPORT FOR ISERIES/AS400 HARDWARE AND SOFTWARE

Innovative Business Systems, Inc.
Joe Gravunder
5218 Comanche Way
Madison, WI 53704
(608) 662-1122 x2
(608) 235-1397
jgravunder@ibs-madison.com
http://ibs-madison.com/

Dorton Technology Solutions, LLC
Chad Dorton
PO Box 275
Kimberly, WI 54136
(920) 570-2750
CHAD.DORTON@DORTONTECHNOLOGY.COM
PRIMARY SERVICES – PROGRAMMING SUPPORT FOR IMS21 SCANNING SOFTWARE

SHI
Michael Vassos
290 Davidson Avenue
Somerset, NJ 08873
888-764-8888
Michael_Vassos@SHI.com
Primary Services – Microsoft Licensing, Equipment ordering

Camera Corner Connecting Point
Camera Corner Connecting Point
529 North Monroe Avenue
Green Bay, WI 54301

Phone Numbers

General Inquiries: (920) 435-5353

Fax Number: (920) 435-6984

Service Dispatch: (920) 438-0333

Network Dispatch: (920) 438-0333

Order Line: (800) 236-4950

NetAssist Team: (920) 438-0337

After Hours Emergency Service:

866-240-5244

Primary Services –Nothing at this time –CCCP did originally install our ShoreTel system

EarthLink/Windstream
Stacy Wielgus
2150 Holmgren Way
Green Bay WI 54304

920-965-7532 office
Stacy.Wielgus@windstream.com
windstreamenterprise.com
Primary Services – Phone Service Provider for Waupaca County (not dispatch, they use AT&T)

TriMin Systems
Erin Hultgren
2277 Hwy 36 West
Suite 250
St. Paul, MN 55113
(855) 636-7667
ERIN.HULTGREN@TRIMINSYSTEMS.COM

PRIMARY SERVICES – SOFTWARE SOLUTIONS FOR COUNTY RECORDERAND REGISTER OF DEEDS

WAUPACA COUNTY
CONTINGENCY PLAN TESTING SCHEDULE

Date of Test	Item (s) Tested (Backup, Restoration, and Etc.)	Test Results	Person Who Performed Test	Date of Next Test

The Contingency Plan must be tested at least once every 180 days.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR
INFORMATION ACCESS MANAGEMENT

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

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule. The organization operates within a larger organization, which is not considered a covered entity under the HIPAA Security Rule. This makes the organization part of a hybrid entity. The organization has adopted this policy to ensure that the covered and non-covered functions implement the necessary controls to allow members of their workforces, with a legitimate need, to have appropriate access to electronic protected health information (ePHI) and to prevent workforce members who do not require access to ePHI to perform their job functions from obtaining such access.

POLICIES AND PROCEDURES

ADEQUATE SEPARATION: FIREWALLS

Included within each designated health care component are various support services including, without limitation, legal, accounting, audit, finance, tax, risk management, information systems management, maintenance, facilities, environmental health and safety. Individuals who perform such support services for both HIPAA health care components and non-covered functions shall not use protected health information that they obtain in the course of furnishing services for the HIPAA covered health care components to provide services to the non-covered functions. In addition, when using or disclosing Protected Health Information, the HIPAA covered health care components shall treat the non-covered functions as if they were legally separate entities.

The non-covered entity must:

1. Describe those employees or classes of employees or other persons under the control of the non-HIPAA covered entity to be given access to protected health information; all employees who receive information in the ordinary course of business must be included in the description.

2. Restrict the access to and use by such employees to administration functions that the non-HIPAA covered entity performs.

3. Provide an effective mechanism for resolving any issues of noncompliance by such employees, including disciplinary sanctions.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR WORKFORCE SECURITY

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

INTRODUCTION

Waupaca County is committed to conducting business in compliance with the HIPAA Security Rule. The organization has adopted this policy to ensure that all workforce members, with a legitimate need, have appropriate access to electronic protected health information (ePHI) and to prevent workforce members who do not require access to ePHI to perform their job functions from obtaining such access.

The organization will ensure that workforce members who work with ePHI or in locations where ePHI is available are appropriately supervised, that workforce members are granted appropriate access to ePHI, and that workforce members' ePHI access is terminated when their employment ends or when a determination is made that such access should be terminated or otherwise modified.

POLICIES AND PROCEDURES

INITIAL GRANT OF EPHI ACCESS AND ONGOING SUPERVISION OF EPHI ACCESS

1. Only workforce members with a need to access ePHI will be granted access to ePHI.

2. The workforce member's supervisor and/or the Security Officer will determine who will require access to ePHI to perform their job functions.

3. The workforce member's supervisor and/or the Security Officer will maintain documentation detailing each workforce member's role and responsibilities, why such workforce members require access to ePHI and the specific levels of ePHI access required by such workforce member.

4. All workforce members who work with ePHI must be supervised so that unauthorized access to EPHI is avoided

ACCESS UPON TRANSFER OF EMPLOYMENT WITHIN THE ORGANIZATION

If a workforce member transfers to another department or workgroup within the organization:

1. The workforce member's access to ePHI within his/her current unit must be terminated as of the date of transfer.

2. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

ACCESS UPON TERMINATION OF EMPLOYMENT

The organization must implement procedures to ensure that when a workforce member's employment terminates:

1. The workforce member's supervisor or manager ensures that all such workforce member's accounts to access ePHI are terminated.

© Copyright 2002-2017, HIPAATraining.com

2. The workforce member's supervisor or manager ensures that such workforce member's access to all facilities housing ePHI is terminated, including but not limited to card access, keys, codes, and other facility access control mechanisms. Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.

3. Human Resources is promptly notified.

4. Access to ePHI is not extended to a workforce member beyond the termination date of such workforce member's employment unless one of the following two conditions have been met:

    - A Business Associate Contract is entered into with such workforce member.
    - The workforce member will be accessing ePHI as in accordance with a HIPAA compliant authorization.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR
INCIDENT RESPONSE AND REPORTING

Category: HIPAA Security (Administrative)	**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 address security incidents.

The scope of this policy and procedure covers the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

POLICIES AND PROCEDURES

REPORTING AND RESPONDING TO HIPAA SECURITY INCIDENTS

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of electronic protected health information (ePHI) must be reported to your immediate supervisor and/or the Security Officer.

The IT department or IT vendor should investigate and propagate recommended updates or fixes to threatened or actual security incidents. The IT department or IT vendor must also notify the HIPAA Security Officer if a threat to ePHI exists.

Each supervisor must report security incidents to the HIPAA Security Officer. Incidents that should be reported include, but are not limited to:

- Virus, worm, or other malicious code attacks
- Network or system intrusions
- Persistent intrusion attempts from a particular entity
- Unauthorized access to ePHI, an ePHI based system, or an ePHI based network
- ePHI data loss due to disaster, failure, or error

The HIPAA Security and Privacy Offices must notify each other of security or privacy issues.

All correspondence with outside authorities such as local police, FBI, media, etc. must go through the Security Officer.

DOCUMENTATION OF SECURITY INCIDENTS

All HIPAA Security related incidents and their outcomes must be logged and documented by the Security Officer.

MITIGATION OF HARMFUL EFFECTS OF KNOWN SECURITY INCIDENTS

The harmful effects of known security incidents will be mitigated by notifying the Security Officer of a known incident so that appropriate action may be taken.

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
SECURITY INCIDENT REPORT - INVESTIGATION FORM

Date of reported concern: _____

Name of person who received the report: _____

Name of person who made the report (state "unknown" if the report was made anonymously):

_____

Date(s) of investigation: _____

Name(s) of person(s) investigating: _____

Name(s) of person(s) interviewed: _____

_____

_____

Description of documents/systems reviewed: _____

_____

_____

Findings: _____

_____

_____

_____

_____

Plan of correction: _____

_____

_____

_____

_____

_____

_____

_____
Signature of Security Officer

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
SECURITY INCIDENT REPORT

The purpose of this form is to report the facts pertaining to any known or suspected violation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule standards or the laws and regulations governing the organization. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the Security Officer at the organization. If you do not want to give your name, you may call the Security Officer within one week of submitting this report to inquire about the outcome of the investigation.

If you wish to identify yourself in this report, the organization will make every effort to keep your identity confidential, unless you give the organization permission to reveal it. Only the Security Officer, and others designated by the Security Officer, will have access to your report. No disciplinary action or retaliation will be taken against you for making a good faith report of a compliance violation.

Please include all the factual details of the suspected violation, however big or small, to ensure that the Security Officer has all of the information necessary to conduct a thorough investigation. Please attach additional pages as needed. The information that you provide should include names, dates, times, places and a detailed description of the incident that led you to believe that a violation of the organization's security standards occurred. Please include a copy or a description of any documents that support your concerns.

Date of this report: _____

Name of person making this report (optional): _____

Description of the violation(s): _____

_____

_____

Detailed description of the incident(s) resulting in the violation (include names, dates, times and places):

_____

_____

_____

_____

_____

Name(s) of person(s) involved in the incident and an explanation of their role:

_____

Name(s) of other person(s) having knowledge of the incident: _____

_____

Department where the incident occurred: _____

_____

© Copyright 2002-2017, HIPAATraining.com

Date(s) of the incident: _____

Explanation of how you became aware of the suspected violation: _____

_____

_____

Please attach or describe any documents that support your concern (include a description of the documents, the identity of the persons who wrote the documents, the dates of the documents, and the location of the documents).

_____

_____

_____

_____

_____

_____

_____

Form should be mailed to:

BRENT WYLAND
811 Harding Street
Waupaca WI, 54981

© Copyright 2002-2017, HIPAATraining.com

WAUPACA COUNTY
POLICIES AND PROCEDURES FOR EMPLOYEE SANCTIONS

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

INTRODUCTION

The purpose of this policy is to address non-compliance with the HIPAA policy requirements governing the confidentiality of electronic protected health information (ePHI).

It is the policy of the organization to take appropriate steps to promote compliance with the requirements for maintaining the confidentiality of ePHI. The organization takes seriously its requirements under HIPAA to protect the confidentiality of ePHI and will respond appropriately to violations of HIPAA policies.

The appropriate response to such violations will depend on the severity of the violation, and the record of the employee.

The response will be decided after investigating the specific facts of the situation and may include, but is not limited to, such actions as: system changes, additional education, a written reprimand, a suspension, and termination of employment.

Employees and others who are working on behalf of the organization, who report, in good faith, violations of HIPAA policy requirements shall not be retaliated against. They may report any retaliation to their direct supervisor, or the Security Officer. If reported to anyone other than the Security Officer, it shall be referred to the Security Officer. The Security Officer shall determine who will investigate the matter.

POLICIES AND PROCEDURES

A. It is the responsibility of the Security Officer to determine the appropriate process to follow when aware of allegations of HIPAA policy violations by an employee. If it is determined that a violation which could result in disciplinary action has occurred, the Security Officer has the responsibility to determine the appropriate response.

B. One of the factors to consider when determining the appropriate response for HIPAA policy violations is the severity of the violation. The organization has determined that there are four categories of violations.

> Type I – these violations are inadvertent or accidental breaches of confidentiality that may or may not result in the actual disclosure of protected health information (for example, sending an email to an incorrect address).
>
> Type II – these violations result from failure to follow existing policies/procedures governing security (for example, failure to obtain appropriate authorization to release information, failure to fulfill training requirements).
>
> Type III – these violations include inappropriately accessing a patient/individual/plan participant's record without a job-related need to know (for example, accessing the record of a friend or co-worker out of curiosity without a legitimate need to know the information).
>
> Type IV – these violations include accessing and using protected health information for personal gain or to harm another person.

C. In addition to the severity of the violation, factors such as the past record of the employee must be considered. As a result, the appropriate response must be determined on a case-by-case basis. For example, while an inadvertent violation might normally result in additional education, it could result in more serious action if it was part of a pattern of violations or other performance problems.

All violations must immediately be reported to the organization's Security Officer.

DOCUMENTATION REQUIREMENTS

Each instance of workforce disciplinary action regarding security of ePHI is to be documented in a written or electronic record by the HIPAA Security Officer. The Sanctions log will contain the following information:

- Name of employee
- Description of violation
- Level of breach or violation
- Location of breach or violation
- Date and time of breach or violation
- Disciplinary action taken

This documentation must be retained for six years from the date of its creation or the date when it was last in effect whichever is later.

WAUPACA COUNTY
Security Sanctions Log

Each instance of workforce disciplinary action regarding security of electronic protected health information (ePHI) is to be documented and reported to the HIPAA Security Officer.

Name of employee	Description of the violation	Level of breach or violation	Location of breach or violation	Date and time of breach or violation	Disciplinary action provided