CONFIDENTIAL

Wake County Medical Society
Community Health Foundation, Inc.

Security Policies

Index of Security Policies

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Background

POLICY #: S1.1

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and, on January 25, 2013, the final omnibus rule modifying the HIPAA privacy and security rules, as outlined in 78 Fed. Reg. 5566 (the "HIPAA/HITECH Omnibus Rule") (collectively, "HIPAA"), the United States Department of Health and Services published detailed federal privacy regulations that protect certain types of health information. These regulations contain a standards that establish: (1) federally mandated requirements regarding how health information can be used and disclosed; (2) individual rights; and (3) administrative requirements, including the adoption of these policies and procedures (the "the Policies and Procedures").

If you require further information or clarification of HIPAA, HITECH and its impact on Wake County Medical Society Community Health Foundation, please contact either your Privacy or Security Officers, who are identified on the WCMSCHF Intranet.

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Definitions

POLICY #: S1.2

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Breach Notification Rule: Breach Notification Rule means the "Breach Notification for Unsecured Protected Health Information" regulations issued by the United States Department of Health and Human Services Office for Civil Rights at 74 Fed. Reg. 42740 (Aug. 24, 2009), and 78 Fed. Reg. 5566 (Jan. 25, 2013), as codified at 45 C.F.R. Part 164, Subpart D.

Business Associate: Business Associate means a person or organization that performs or assists in the performance of certain functions, activities, or services on behalf of a Covered Entity that involves creating, receiving, maintaining, or transmitting PHI. A Business Associate includes any agent or subcontractor of a Business Associate that creates, receives, maintains, or transmits PHI on behalf of the Business Associate, other than in the capacity of a member of the Workforce of such Business Associate. WCMSCHF often functions as a Business Associate.

Business Associates include (but are not limited to): A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to Protected Health Information to a Covered Entity and that requires access on a routine basis to such Protected Health Information, a person or entity that offers a personal health record to one or more Individuals on behalf of a Covered Entity; a subcontractor that creates, receives, maintains or transmits Protected Health Information on behalf of the Business Associate.

Examples of such functions, activities, or services include: data analysis, processing, or administration; website hosting; utilization review; quality assurance; patient safety activities (listed at 42 C.F.R. § 3.20); billing; collections; benefit management; practice management; repricing; legal services; actuarial services; accounting and auditing services; consulting; data aggregation; management and administrative services; accreditation; financial services; or any other service in which the person or organization obtains PHI from or on behalf of a Covered Entity or another Business Associate. Employees are not considered Business Associates of WCMSCHF.

The exchange of PHI between providers of health care, for purposes of providing Treatment to a patient, does not create a business associate relationship.

Business Associate Agreement: Business Associate Agreement means a contract between and Business Associate and a Covered Entity pursuant to 45 C.F.R. § 164.504(e).

Covered Entity: Covered Entity has the same meaning as the term "Covered Entity" set forth at 45 C.F.R. § 160.103, and includes: a health plan, a healthcare clearinghouse, or a healthcare provider that conducts electronic transactions for which HIPAA standard transactions have been adopted. As of the Effective Date of these Policies and Procedures, WCMSCHF does not function as a Covered Entity.

Disclose or Disclosure: Disclose or Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Electronic Media: Electronic Media means:

- Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and

- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic PHI or EPHI: Electronic PHI means PHI transmitted or maintained in Electronic Media. This includes e-mail, text, or any form of transmission where PHI is in an electronic medium.

Employees: Employees means, solely with respect to these Policies and Procedures, any member of WCMSCHF's Workforce, including employees, volunteers, trainees, interns, and temporary staff, and other persons whose conduct, in the performance of work for WCMSCHF, is under the direct control of WCMSCHF, whether or not they are paid by WCMSCHF.

HIPAA Privacy Rule: HIPAA Privacy Rule means the "Standards for Privacy of Individually Identifiable Health Information" set forth at 45 C.F.R. Parts 160 and 164, Subparts A and E.

HIPAA Security Rule: HIPAA Security Rule means the "Security Standards" set forth at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Individual: Individual means the person who is the subject of PHI and includes persons who are living or those who are deceased for 50 years or less.

Individually Identifiable Health Information: Individually Identifiable Health Information means that subset of health information, including demographic information collected from an Individual, that:

- Is created by or received by a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future Payment for the provision of health care to an Individual; and
- That identifies the Individual or with respect to which there is a reasonable basis to believe that information could be used to identify the Individual.

Information Technology Department: Information Technology Departments means WCMSCHF's information technology department, the members of which are identified on the WCMSCHF Intranet Staff Directory.

Policies and Procedures: Policies and Procedures mean these Security Policies and Procedures.

Protected Health Information or PHI: Protected Health Information means Individually Identifiable Health Information transmitted or maintained in any format (written, electronic, or oral), relating to an Individual (meaning, those who are living or who have been deceased for 50 years or less).

Privacy Officer: The individual with WCMSCHF that holds the title of HIPAA Privacy Officer, identified on WCMSCHF's Intranet.

Security Officer: The individual with WCMSCHF that holds the title of HIPAA Compliance and Security Officer, identified in Policy S1.4.

Standard Operating Procedures: Standard Operating Procedures means those operating procedures that apply to a specific arrangement or project, as determined by the Security Officer.

Use: Use means the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains the information.

WCMSCHF: WCMSCHF means Wake County Medical Society Community Health Foundation, Inc.

Workforce: Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Purpose and Scope

POLICY #: S1.3

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose: The Purpose and Scope Policy defines the purpose and scope of the WCMSCHF's Security Policies and Procedures.

Synopsis: The HIPAA Security Rule applies to Covered Entities and Business Associates. As an entity that performs certain functions on behalf of Covered Entities, WCMSCHF functions as a HIPAA Business Associate. This policy serves to help Employees understand why these Policies and Procedures have been put into place and WCMSCHF's role in protecting the security of EPHI.

Policy:

<u>Status as Business Associate</u>

The HIPAA Security Rule protects the confidentiality, integrity, and availability of PHI held or transferred in electronic form. Although WCMSCHF is not a Covered Entity within the meaning of the Security Rule, WCMSCHF is a Business Associate of Covered Entities, as WCMSCHF may create, receive, maintain, or transmit EPHI from Covered Entities in WCMSCHF's performance of services on behalf of such Covered Entities.

As a result of the HITECH Act, WCMSCHF, as a Business Associate, must directly comply with certain provisions of the HIPAA Privacy Rule and HIPAA Security Rule, and the Breach Notification Rule. WCMSCHF may be subject to civil monetary penalties for failure to comply with such regulations. In order to ensure compliance with the HIPAA Security Rule, WCMSCHF is implementing these Policies and Procedures to govern the security of Electronic PHI received from, or created, maintained or transmitted by WCMSCHF on behalf of, Covered Entities.

<u>Applicability to Employees</u>

All Employees are required to follow these Policies and Procedures as they apply to their activities within WCMSCHF when creating, using, maintaining, or transmitting Electronic PHI. Questions about these Policies and Procedures should be referred to the Security Officer.

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Designation of HIPAA Security Official

POLICY #: S1.4

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(2)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

This policy is based on the need to designate an official from WCMSCHF who will perform the role of HIPAA Security Officer. The designated official will undertake the responsibility of oversight of all activities involving EPHI and the necessary security safeguards.

Synopsis:

We are required to designate someone who will be the Security Officer and oversee the implementation and maintenance of safeguards that will protect EPHI. These safeguards could be administrative such as policies and procedures, or technical such as access control to computer systems and resources, or physical such as limiting access via locks. The Security Officer must also make Employees aware of these safeguards and their use, and review, modify and implement new safeguards when needed. Please see the Security Officer's job description, maintained by the Human Resources Department.

Policy:

- WCMSCHF will designate a Security Officer who will perform the necessary functions to protect the confidentiality, integrity, and availability of EPHI in accordance with 45 C.F.R. § 164.308(a)(2).
- The Security Officer is responsible for the development and implementation of policies and procedures to safeguard privacy and security of EPHI.
- The Security Officer will maintain and review the policies on a yearly basis and when information technology ("IT") and business environment changes demand a review.
- The Security Officer will monitor the implementation of the policies and the training of Employees regarding those policies.
- The Security Officer will be responsible for HIPAA security training for Employees so they can effectively perform their job functions.
- The Security Officer will be the contact person regarding matters of security, access control, and the implementation of new technologies.

- As of the effective date of this policy, Hazen Weber is the designated Security Officer for WCMSCHF. The designated Security Officer may be changed from time to time, and any such change will be communicated to Employees by email and through announcement at the next all staff meeting.

Related Documents:

- Privacy Officer P1.4

Revision History:

Created: September 6, 2012 by Hazen Weber
Approved: September 7, 2012 by Susan Davis

Revised: September 6, 2013 by Hazen Weber
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Hazen Weber
Approved: July 28, 2014 by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Workforce Clearance/Background Check Policy

POLICY #: S2.1

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(3)(ii)(B)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
To address the establishment of workforce clearance procedures for workforce members who have access to EPHI, including background checks and drug testing.

Synopsis:
WCMSCHF is responsible for taking certain steps to vet Employees before granting Employees access to PHI, authenticating the need for access to PHI, and approving requests to access EPHI. This policy explains how WCMSCHF fulfills these requirements.

Policy:

- WCMSCHF has processes in place as specified in the Employee Handbook to conduct checks on credit, criminal and driving histories for candidates prior to hiring.
- Section 6 (Employee Access to PHI) of the Master Policy (P1.1) addresses job categories that need access to PHI, and Security Policy S2.7 (Access Control and Logging Policy) specifies how access to PHI/EPHI can be requested by authorized supervisors.
- The Information Technology Department maintains written procedures that dictate how access to EPHI systems may be granted, and how access requests are stored electronically as a record.

Related Policies and Documents:

- WCMSCHF Employee Handbook (Located on WCMSCHF Intranet)

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Acceptable Use Policy

POLICY #: S2.2

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.310(b), 164.310(c), 164.312(a)(2)(iii)

NCQA STANDARD: B.3, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to outline the acceptable use of computing assets at WCMSCHF. These rules are in place to protect the WCMSCHF system users and WCMSCHF. Inappropriate use exposes WCMSCHF to risks that could compromise network systems and services, and lead to legal recourse.

Synopsis:
WCMSCHF provides each Employee and those working on behalf of WCMSCHF with the resources they require to fulfill the function of their respective jobs. Individuals utilizing WCMSCHF resources have an obligation to utilize those resources in a responsible manner, being mindful of WCMSCHF interests, and the interests of those with whom WCMSCHF partners. This policy sets forth the requirements for those that utilize WCMSCHF resources and specifies both acceptable and unacceptable means of use.

Scope:
This policy applies to all computing assets that are owned or leased by WCMSCHF and/or are accessed through WCMSCHF's network. Employees are responsible for extending the terms of this policy to contractors, consultants, temporaries, and other third parties accessing WCMSCHF systems or networks through execution of the Visitor Confidentiality Agreement.

Policy:

General Use and Ownership

- All network resources provided by WCMSCHF (including internal and external resources) as well as computer equipment, software, and peripherals are the property of WCMSCHF and are to be used for business purposes only, except as described below.

- All devices, software, books, training materials, documentation and any other approved purchases that Employees are reimbursed for by WCMSCHF are the property of WCMSCHF.
- All data stored on WCMSCHF devices is the property of WCMSCHF, and Employees are not entitled to privacy regarding information stored on or accessed by WCMSCHF devices.
- WCMSCHF reserves the right to monitor and audit WCMSCHF equipment and systems, as well as access equipment and systems for security and maintenance purposes. All information transmitted on or from, received or accessed by, or residing on the equipment and systems may be monitored and read by WCMSCHF at its discretion, even if it is information that is understood by the user to be private and confidential. Use of such equipment and systems constitutes express consent to WCMSCHF's monitoring of and access to the information therein.
- Personal use of WCMSCHF resources must be minimal, reasonable, and not destructive nor compromise WCMSCHF, its systems or data, nor violate any WCMSCHF policies. Personal use of WCMSCHF's systems may be audited and monitored in accordance with these Policies and Procedures.

Security and Proprietary Information

- Systems users will be active in protecting WCMSCHF resources and preventing unauthorized access by:
  - Complying with password policies and requirements.
  - Locking workstations when leaving them, and logging off at the end of the day.
  - Complying with email and encryption policies especially regarding the transmission of EPHI.
  - Complying with all anti-malware policies
- Sensitive and confidential information and PHI will not be posted on unsecured websites, or unaffiliated web-based sites or systems.
- Users must report any weaknesses in or concerns about WCMSCHF systems security to the Security Officer or the Information Technology Department.
- Users must report any attempts of unauthorized access such as unsolicited support calls regarding their computer systems, WCMSCHF systems, or websites.

Unacceptable Use

The following actions and activities are prohibited:

- Utilizing WCMSCHF resources in ways other than intended or approved, and in violation of any WCMSCHF documented policy or procedure.
- Utilizing WCMSCHF resources in a way that degrades system performance such as streaming music and videos unrelated to your job function.
- Accessing WCMSCHF resources, information or data in an unauthorized manner.
- Any illegal activity including but not limited to copyright infringement, violations regarding intellectual property, the installation and distribution of illegal or "pirated" software products, or unauthorized duplications of software.
- Utilizing unauthorized file-sharing applications (e.g. LimeWire, Bit-Torrent), installing unapproved applications, or utilizing unauthorized web-based applications to house WCMSCHF related data.
- Intentional introduction of malicious programs to the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs etc.)

- Revealing your account password to others or allowing the use of your account by others.
- Using a WCMSCHF computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Falsely representing WCMSCHF, or speaking on behalf of WCMSCHF unless authorized, or making fraudulent offers of services.
- Accessing systems in an unauthorized manner, and accessing systems/resources in efforts to undermine, manipulate damage, destroy or block access such as a denial of service attack.
- Utilizing WCMSCHF for personal benefit or gain, political activities, unsolicited advertising or fundraising, or the solicitation or performance of any activity that is prohibited by local, state or federal law.
- Non-compliance with existing policies.
- Divulging PHI except as expressly permitted by WCMSCHF policies and procedures.
- Divulging trade secrets, private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not divulge PHI, internal reports, policies, procedures or other internal business-related confidential communications.
- Violating copyright and other intellectual property laws. For WCMSCHF's protection as well as your own, it is critical that you show proper respect for the laws governing copyright, the fair use of copyrighted material owned by others, trademarks and other intellectual property, including WCMSCHF's copyrights, trademarks, and brands.
- Please note that nothing in this policy is designed to interfere with, restrain, or prevent employee communications regarding wages, hours, or other terms and conditions of employment. Employees have the right to engage in or refrain from such activities.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15)

Standards:

Related Documents:

- Password Policy (S2.8)
- Email Policy (S2.9)
- Acceptable Encryption Policy (S2.11)
- Security Incident Response Plan (S3.2)
- Privacy Master Policy (P1.1)
- Social Media Policy (P1.13)

Revision History:

Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 19, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: IT Physical Asset Policy

POLICY #: S2.3

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. §§ 164.310(c); 164.310(d)(2)(iii)

NCQA STANDARD: A.4, B.3, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy is based upon the control entitled, "Establish and maintain physical security for distributed IT assets". IT assets such as computers, printers, routers and the like are located in remote locations and cannot be easily controlled. Therefore, WCMSCHF has developed procedures and practices for protecting those distributed assets wherever they may be found to ensure that only properly authorized access is allowed.

Synopsis:
Information Technology based assets are both critical to our function as an organization and are expensive. Loss or damage to these assets could negatively affect your ability to function within your role and could subject WCMSCHF to HIPAA/HITECH compliance concerns. This policy specifies how the Information Technology Department staff will work to control and monitor WCMSCHF's inventory, and how Employees can best support this effort in protecting our assets.

Policy:

- Employees will be made aware of all policies governing the use of WCMSCHF assets and will be properly trained to use these devices within their role.
- WCMSCHF shall implement standards for home office locations to safeguard WCMSCHF assets.
- WCMSCHF will implement standards for destroying sensitive information no longer needed and where applicable the reuse of media after destroying information.
- WCMSCHF shall implement procedures that govern the receipt and removal of assets provided to Employees upon their joining and leaving the organization.
- The Information Technology Department will maintain an inventory and review and update inventory records every six months, or more frequently as needed.

- The inventory will include assets critical to the storage and transmission of EPHI, and all other electronic devices that store or transmit EPHI, including without limitation computers, servers, printers, and other Electronic Media.
- Hardware changes, maintenance made to server-centric or network infrastructure devices and Electronic Media will be documented, and the inventory will be updated as appropriate at the time of such change or maintenance.
- Approved IT assets capable of connecting to WCMSCHF's network within WCMSCHF's main office spaces will be connected via a wired connection or secured wireless connection within the facility premises.
- Unauthorized devices are not allowed to connect to the WCMSCHF network.
- WCMSCHF IT assets will be governed by the policies of access and security specifically implemented for the particular device.

Workstation Requirements:

- WCMSCHF will adopt the following physical and technical security safeguards for all workstations that access EPHI:
    - When possible, all workstations should be located within an office environment away from areas accessible to the public.
    - Fixed workstations in public areas must utilize privacy screens, should be locked when left unattended and should be powered off when unattended overnight or for long periods of time.
    - Access to workstations will be limited to those Employees authorized to access EPHI in accordance with the Access Control and Logging Policy (S2.7).
    - Employees using a WCMSCHF workstation will be mindful of PHI and sensitive information that they access or utilize in performing their job function, and will only access or utilize PHI in accordance with WCMSCHF policies and procedures and applicable law.
    - Employees will restrict access to their computer systems from unauthorized users including family, friends, and unauthorized co-workers.
    - Employees will secure the computer by locking or logging off the computer prior to leaving the work area.
    - Workstations will be configured to utilize password protected screen savers after 10 minutes of inactivity.
    - Be aware of PHI on monitors when in publicly accessible areas to avoid unintentional viewing of PHI in accordance with the Clean Desk Policy.
    - Store all sensitive information, including EPHI on network servers in an appropriately secure location and a manner consistent with the access rights outlined in Section 6 (Employee Access to PHI) of the Privacy Master Policy (P1.1).
    - Keep food and drink away from workstations to avoid accidental spills and damage.

Disposal of EPHI

- WCMSCHF and Employees will dispose of EPHI and reuse Electronic Media as follows:
    - Employees should not destroy or dispose of Electronic Media without the prior approval of the Security Officer.

  - The Security Officer is responsible for overseeing the proper disposal of EPHI, including all Electronic Media containing any EPHI and the reuse of any Electronic Media in accordance with WCMSCHF policies and procedures.
  - Individual files containing PHI located on computers should be erased using an Information Technology Department approved secure deletion/erasing program.
  - Electronic Media being destroyed, disposed of, or reused will be securely wiped using the then current standards required by the Information Technology Department, which shall not be less than the industry standards, and when necessary physically destroyed, before leaving the possession of WCMSCHF and before being returned to a vendor.

- The destruction, disposal, and reuse of all Electronic Media will be documented by the Security Officer in accordance with these Policies and Procedures.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15)

Standards:

- WCMSCHF Inventory Standards Document
- Asset Inventory Procedure
- Secure Deletion of PHI Procedures Document

Related Documents:

- Access Control and Logging Policy
- Password Policy
- Acceptable Use Policy
- Anti-Malware Policy
- Acceptable Encryption Policy
- Wireless Access Policy
- Clean Desk Policy

Related Standard Operating Procedures:

- Inventory Maintenance Log
- Inventory Asset Database
- Server-Closet Maintenance Logging Procedures

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 19, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Physical Security Policy

POLICY #: S2.4

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.310(a)(2)(ii)

NCQA STANDARD: B.1, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy is established to define the requirements for physical and environmental security at WCMSCHF offices and home office locations that involve access to, use, or disclosure of EPHI. These are designed to safeguard our Employees and the property and information maintained by WCMSCHF from unauthorized physical access, tampering, and theft.

Synopsis:
Given the type of information we work with and store, we have to implement physical measures such as locks and smoke detectors to help ensure the safety of our people, our data, and IT resources.

Policy:

Physical Access Control (Main Offices)

- Proximity readers are located at the buildings main and side (near garage) entrances to restrict after-hours access to the premises.
- The rear door near the Information Technology department is not for regular entrance and is secured by a keyed lock.
- Punch-code locks will be installed on the main and side (near garage) entrances of the office suite.
- Punch-code locks will have their code changed in the event of an involuntary termination of employment, or more frequently as determined by the Security Officer.
- Visitors must be let into the office and then secured as defined within the Visitor Access Policy (S2.6).
- Changes or modifications including repairs on locks and doors within the WCMSCHF premises will be documented.
- Bi-annual inspections will be conducted by the Security and Privacy Officers and recommendations will be submitted to senior management.

Power Protections and Environmental Controls (Main Offices)

- Servers and network equipment will be equipped with an Uninterruptable Power Supply (UPS) and access to these systems will be restricted.
- Smoke detectors and fire alarms will be present throughout the main office locations in compliance with applicable building codes.
- At least one fire extinguisher will be present in a centralized location in each main office location.
- Emergency exit information will be posted in an obvious manner, and Employees will be made aware of the exit strategy.
- Bi-annual inspections will be conducted by the Security and Privacy Officers to evaluate compliance.

Property Controls (Main Offices)

- Movement of any server-side or network infrastructure hardware must be done with the knowledge and approval of the Information Technology Department Manager and with the assistance of the Information Technology Department.
- Servers will be maintained within a restricted location with access limited to only essential personnel.
- Movement of any workstations or laptop/workstation workspaces within the main office environment must be done with the knowledge of the Information Technology Department.
- Documentation of all server-side hardware movements must be maintained including data storing peripherals.

Physical Access and Environmental Controls (Home Offices)

- Employees with home offices will use best efforts to restrict access to their home offices.
- In the event that non-Employees will be entering the home office location, WCMSCHF related PHI and EPHI must be secured and out of view.
- Employees with home offices will maintain at least one smoke detector on each floor of their home, with one smoke detector located near the home office.
- Employees will utilize surge protected power strips for all WCMSCHF provided equipment.
- Employees using wireless internet from a home office must comply with WCMSCHF’s Wireless Security Policy (S2.12).
- Employees are required to complete the Home Office Assessment Authorization Form, and the signed form will be stored in their electronic staff profile. The current Home Office Assessment Authorization Form is maintained by the Security Officer. Please see the Security Officer for the current version.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15)

Standards:

Related Documents:

- Wireless Security Policy
- Visitor Access Policy

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 23, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 19, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Keys and Access Card Policy

POLICY #: S2.5

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.310(a)(2)(ii)

NCQA STANDARD: B4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:

This policy is designed to specify the means by which keys and key card access can be requested, distributed, and revoked, and who maintains the keycard access systems.

Policy:

- Certain WCMSCHF facilities will be restricted to individuals by use of keys and keycard access.
- The WCMSCHF office requires keycard access after reasonable work hours, on a schedule set by the building supervisor, in order to enter the building.
- The building supervisor configures keycard access, maintains the keycard access system, and manages logs in compliance with their own policies. The building supervisor and the keycard access system are outside the scope of WCMSCHF control.
- Requests to grant or revoke a key or keycard will be submitted only by managers and utilizing the appropriate request form approved by the Security Officer.
- The Information Technology Department is responsible for storing all key and keycard access request forms.
- The Information Technology Department will forward all applicable documentation to the Human Resources Department who will obtain and distribute both keys and keycards.
- Human Resources will maintain an audit log of keys and keycards provided to Employees and will review the appropriateness of authorized access yearly.
- Human Resources will recover and/or terminate key and keycard access upon termination of an Employee’s employment or upon request from the Employee’s manager.
- Lost keys and keycards must be reported to the Information Technology Department and Human Resources**.**

- In the event of an investigation, the Security Officer will request information if pertinent from the building supervisor regarding any entry and keycard use logs if such logs are available.
- The rekeying of locks, access card systems and punch codes due to security concerns will be implemented by the Human Resources department and/or the Security Officer.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:

Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 19, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Visitor Access Policy

POLICY #: S2.6

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to guide Employees hosting professional guests at an office location and entertaining personal guests within the home office environment.

Synopsis:
You have access to an abundant amount of PHI and we need to ensure that such PHI is kept protected. At the same time, we as an organization often work with partner organizations and may have visitors within the main office space. Also, Employees with home-based offices may have personal guests within their home. A visitor's proximity to PHI makes them a higher risk, and so this policy governs how to address visitors.

Policy:

- Visitor Registry: Visitors to the office must sign the Visitor Registry. It is the responsibility of the Employee hosting the guest to have them sign the Visitor Registry. The Visitor Registry will be collected at the end of the month and stored electronically on an approved system.
- Visitor Confidentiality Agreement: In addition to signing the Visitor Registry, all visitors must review and sign the "Visitor Confidentiality Agreement". A current version of the Visitor Confidentiality Agreement is located on the Intranet's main page. Please send signed copies of the "Visitor Confidentiality Form" to Tara Kinard (Privacy Officer) on the day of the visit.
- Visitors will be greeted upon entering, not be left alone or allowed to roam within the main office environment. Visitors must be accompanied by an Employee host until they have left the office suite. A visitor cannot sponsor another visitor.
- If an Employee observes an unknown individual within the main office environment, they should introduce themselves, and address the individual to determine their need and their reason for visiting.

- Visitors are not permitted to take photographs or videos within the premise of WCMSCHF, unless discussed and approved by WCMSCHF management. Access to WCMSCHF resources, including wireless network systems (WLAN), and cabled network access (LAN) are by default restricted.
- If a visitor requires Internet access they may be provided with wireless access information for the guest network by the host Employee in accordance with the Wireless Security Policy (S2.12), but the access should be removed from their device when their need or visit concludes.
- Employees entertaining guests within their home must ensure that WCMSCHF resources on the premise are restricted from being accessed by guests, and all PHI is out of sight and secured.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Documents:

- Privacy Master Policy (P1.1)

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 19, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Access Control and Logging Policy

POLICY #: S2.7

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(D), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(iii), 164.312(d)

NCQA STANDARD: A.2, A.10, B.3, B.5, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy is based upon the Control entitled, "Establish and maintain access policies and access procedures". The purpose of this policy is twofold; 1.) to establish an identification, authentication and user rights plan for both internal and externally maintained systems, and 2.) to log the activities of that plan.

Synopsis:
We provide access to resources and information, but only to the extent access is required for a person to fulfill his or her job function. Furthermore, we need to have a process that states how access to PHI should be requested (by your manager), implemented (Information Technology Department), and logged (Security Officer). This Access Control and Logging Policy explains who can approve systems access and the means to request that access, and how it is logged.

Policy:

- Access to PHI should be limited to the extent relevant to the work role / job function, and can only be requested by those in authority over the individual and/or the Executive Director.
- Requests for access should follow the principle of "minimum necessary", described in Section 7 (Permitted Uses and Disclosures of PHI) of the Privacy Master Policy (P1.1) and should be based on the amount of information needed for the Employee to perform his or her job function as described in Section 6 (the Employee Access to PHI) of the Privacy Master Policy (P1.1).
- Requests and changes in access will be made using the appropriate access form and will be stored electronically in the Employee's staff profile.

- All requests must be approved by Employee’s manager in accordance with Section 6 (Employee Access to PHI) of the Privacy Master Policy (P1.1). Upon such approval, the Information Technology Department will implement the technical changes to give Employee access to PHI.
- Employees will access network resources and especially PHI via an individualized authentication process or account.
- In the event that an account is created for a specific role or job function (as opposed to a user specific account), and an individual is assigned to that account for a limited period of time, the password for the account will be changed prior to granting another individual access to the account. Only one individual will have access to such an account at any time.
- Access granted to PHI will be logged and reviewed and modified as necessary, with changes stored electronically in the Employee’s profile.
- When an Employee changes roles, the staff member’s new manager will promptly notify the Information Technology Department of the staff member’s new role using the appropriate access forms. Upon receipt, all access will be promptly denied, and new access rights will be assigned based on the request submitted by the acting manager of the new role.
- Upon termination of employment or suspension of an Employee, access to internal systems containing PHI will be immediately terminated. Also, notification of account termination will be immediately made to appropriate entities who maintain any external systems that the Employee may have access to.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Policies and Procedures:

- User Identification and Account Standards
- Access Request Change Procedure
- Access Request Termination Procedure
- New Hire Access Request Procedure

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Password Policy

POLICY #: S2.8

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(4)

NCQA STANDARD: B.2, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:

Passwords are an important aspect of computer security. They are the front line for the protection of user accounts. A poorly chosen password may result in the compromise of WCMSCHF's entire network. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency passwords must be changed as specified by the Security Officer and the Information Technology Department.

Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any WCMSCHF facility, has access to the WCMSCHF network, or stores any non-public WCMSCHF information.

Policy:

General

- All passwords should be kept secure, with authorized users responsible for the security of their passwords and accounts.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at defined regular intervals as specified by the WCMSCHF IT Department in a Standard Operating Procedure for systems controlled by WCMSCHF.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Password-protected screensavers will be utilized on all desktop and laptop computers and set to activate after 10 minutes of inactivity.
- VPN system passwords must be changed at defined regular intervals as specified by the WCMSCHF IT Department in a Standard Operating Procedure.
- Employees will have the option to change their password at any given time.

- All user-level and system-level passwords must conform to the password complexity requirements, password protection standards, and other standards specified in a Standard Operating Procedure.
- Employee passwords for WCMSCHF systems should not be utilized for personal accounts.
- If the Employee suspects that a password has been compromised contact the WCMSCHF Information Technology Department immediately.
- The Information Technology Department may perform password cracking tests on WCMSCHF accounts and systems to determine the strength and security of Employee's passwords.

IT Related Accounts

- All administrative system-level passwords (e.g., root, enable, application administration accounts, etc.) will be maintained and updated as specified by the WCMSCHF IT Department in a Standard Operating Procedure.
- All administrative system-level passwords must be securely documented and stored in an appropriately restricted location.
- The Information Technology Department should not share passwords with external support or vendors without permission of Information Technology Department management.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Documents:

Revision History:

Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Hazen Weber

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Email Policy

POLICY #: S2.9

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: B.2, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy serves to protect WCMSCHF from data theft, inadvertent distribution, unauthorized use of email, and risk of damage by malware.

Synopsis:
We provide our Employees with access to email for business use. Email is very convenient, but also carries with it some risks, such as sending PHI in an unsecured way to a non-wakedocs.org address. Also, email is a way of obtaining malware applications that can disrupt your computer's function. This policy tells you how to guard against some of these risks, and what is deemed acceptable and unacceptable with regards to email use.

Policy

Prohibited Use

- No email containing PHI will be sent outside of the WCMSCHF network (i.e. to an email address not ending in @wakedocs.org) without encryption tools and protections approved by the Information Technology Department.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.
- Knowingly sending viruses, spyware or any type of malicious software or code is prohibited.
- Any form of harassment via email, whether through language, frequency, or size of messages is prohibited.
- Unauthorized use, or forging, of email header information is prohibited.
- Solicitation of email or any other email address, other than that of the poster's account, with the intent to harass or collect replies is prohibited.

- Use of unsolicited email originating from within WCMSCHF's networks or other Network/lnternet/lntranet/Extranet service providers on behalf of, or to advertise, any service hosted by WCMSCHF or connected via WCMSCHF's network is prohibited.
- Posting the same or similar non-business-related message to large numbers of Usenet newsgroups (newsgroup spam) is prohibited.

Personal Use

Personal use of WCMSCHF email must be minimal, reasonable, and not destructive nor compromise WCMSCHF, its systems or data, nor violate any WCMSCHF policies.

Monitoring

WCMSCHF employees shall have no expectation of privacy in anything they store, send, or receive on the company’s email system. WCMSCHF may monitor messages without prior notice, though WCMSCHF is not obliged to monitor email messages.

Email Retention

- WCMSCHF does not have a global policy regarding email retention.
- In the event of a breach or certain legal concerns (like a “litigation hold”), all emails regarding the subject matter must be retained in a secure and confidential manner. Contact the HIPAA Security Officer for assistance.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Documents:

Revision History:

Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 23, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy (This policy should be rescinded as we no longer allow PCD's on our network. Any other areas are covered under other policies.

POLICY TITLE: Personal Communication Devices Policy

POLICY #: S2.10

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(4)

NCQA STANDARD: B.2, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
This document describes requirements for Personal Communication Devices for WCMSCHF.

Synopsis:
This policy applies to any use of Personal Communication Devices ("PCDs"), such as iPads, PDA's or Smart Phones (i.e. iPhone, Blackberry, Palm, Droid) to access WCMSCHF data. This does not prohibit staff from connecting their personal phones or tablet devices to WCMSCHF's guest wireless network. But because email and calendaring data may contain PHI it is important that certain security measures are taken, and adhered to, in order to ensure the protection of that PHI.

Policy:
Effective October 1, 2016, Personal Communication Devices that are owned by the employee rather than WCMSCHF, will no longer be allowed to access WCMSCHF network data. Only devices provided by WCMSCHF may be allowed to access email and other network storage data.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

- Personal Communication Device Authorization Form

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Acceptable Encryption Policy

POLICY #: S2.11

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii)

NCQA STANDARD: B.2, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to provide guidance in the types of encryption that can be utilized at WCMSCHF, and the federal restrictions to send encryption technologies outside of the United States.

Scope:
Encryption is a technology we can use to protect sensitive information such as PHI. There are various types of encryption, some better than others, and various ways it can be implemented. This policy discusses some approved ways to encrypt data. Always check with the Information Technology Department if you have any questions.

Policy:

Issuing Policy

- Only encryption that is approved by the Information Technology Department can be utilized to protect data in the possession of Employees.
- Encrypted data (or unencrypted EPHI) cannot be sent outside of the United States, nor should any application, free or otherwise, used to encrypt data be sent outside of the United States without the Security Officer's approval.

Approved Use of Encryption

Encrypted Documents

Documents created with Microsoft Word or Microsoft Excel 2007 or later can be encrypted utilizing the Microsoft's integrated encryption solution per the WCMSCHF Encryption Standards Document.

Documents created with Adobe Acrobat can be encrypted utilizing Adobe's built-in AES encryption.

Encrypted Hard Drives
All laptop and desktop computer hard drives must be encrypted with an encryption algorithm determined appropriate and provided by the Information Technology Department.

Encrypted Portable Media
Portable media, such as USB memory devices, must be provided by the WCMSCHF Information Technology Department. All portable media must be encrypted as determined appropriate and provided by the Information Technology Department (such as IronKey).

Encrypted FTP Transfers
FTP transfers of data, both inbound and outbound, will fall under the encryption requirements specified within in the FTP Connection Policy (S5.7).

Encrypted VPN Connection
VPN Connections to WCMSCHF resources must be encrypted utilizing the technologies and means provided by the Information Technology Department.

Encrypted Email
All emails that contain PHI or confidential information pertaining to WCMSCHF must be encrypted using technologies and means approved by the Information Technology Department before leaving the WCMSCHF network, as specified by the Email Policy (S2.9).

Additional Encryption Techniques
If a need for the encryption of a document type or connection not specifically mentioned within this policy is required, the Information Technology Department should be contacted to recommend and/or approve an appropriate means of encryption information.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

- WCMSCHF Encryption Standards Document

Related Documents:

- Removable Media Policy
- FTP Connection Policy

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Wireless Security Policy

POLICY #: S2.12

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: B.2, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:

The purpose of this policy is to specify the responsibilities of Employees in managing and accessing WCMSCHF wireless networks, and wireless networks not controlled by WCMSCHF.

Synopsis:

Wireless access is prevalent and prone to attacks. These attacks happen most often on unsecured networks. WCMSCHF installs or configures secure wireless network connections at the main office and the home office of any Employee. However, in external offices and meeting places, wireless may not be secured. This policy helps you understand the threats of an unsecured wireless network and how to be secure in using wireless connections with our resources.

Policy:

General Requirements

- All Employees must utilize when available approved WCMSCHF wireless access points or WCMSCHF wireless access provided to them by the Information Technology Department when accessing WCMSCHF data resources.
- Only WCMSCHF provided devices may connect to the WCMSCHF Office wireless network, unless authorized by the Information Technology Department. All guest and non-WCMSCHF provided devices should connect to the WCMSCHF Guest wireless system for Internet access.
- Employees may not reconfigure, or undermine any wireless access device.
- If the wireless device does not seem to function as implemented, Employees will immediately contact the Information Technology Department.
- If Employees are concerned for any reason about the security of a wireless access point, provided by WCMSCHF or otherwise, they should contact the Information Technology Department.

- Employees should only share WCMSCHF controlled wireless access with those individuals they trust and in accordance with the Visitor Access Policy.

Connection to Wireless Networks Not Supported By WCMSCHF

- Caution should be used when accessing wireless networks not controlled by WCMSCHF.
- If possible do not utilize wireless networks that are not configured with a password to secure access.
- If you must connect to a wireless network that is not secured, it is the responsibility of the Employee to ensure that all communications are done through secure means either via VPN connection to WCMS, or SSL encrypted web portals, and to remain connected only as long as necessary.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

- Visitor Access Policy

Revision History:

Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Virtual Private Network Policy

POLICY #: S2.13

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: B.2, B.4, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:

The purpose of this policy is to provide guidelines for Remote Access VPN connections to the WCMSCHF corporate network.

Synopsis

A virtual private network (VPN) is what allows your WCMSCHF computer to access network resources as if it were working from the main office. VPNs are helpful, but because they allow access to our network they must be configured properly and used with care, otherwise unauthorized access could occur, or data transmitted over the VPN could be sent in an insecure manner. This policy governs WCMSCHF configured VPN connections.

Policy:

Approved WCMSCHF employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating the installation of high-speed internet, and maintaining passwords required for access. Configuration of the VPN access will be completed, approved, and secured as recommend by the Security Officer and the Information Technology Department

Statement of Requirements:

General Requirements

The following requirements must be met by all individuals utilizing the WCMSCHF VPN connection unless specified otherwise in writing prior to implementation by the Information Technology Manager.

- It is the responsibility of each employee with VPN privileges to ensure that unauthorized users do not gain access to the authorized employee’s VPN password or otherwise gain access to WCMSCHF internal networks through the authorized employee’s VPN connection.

- VPN use is to be controlled using the authentication strategy implemented by the Information Technology Department, and must be adhered to at all times.
- When actively connected to the corporate network, VPNs will limit traffic to and from WCMSCHF resources to authorized systems.
- Connection to secondary networks via a second VPN connection established after the original VPN connection to WCMSCHF is established is not allowed.
- VPN gateways will be set up and managed by the WCMSCHF Information Technology Department.
- All computers connected to WCMSCHF internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the WCMSCHF standard.
- Users are not to remain connected to WCMSCHF via the VPN connection while the connection is not in active use. This means users should disconnect from the VPN connection when access to those resources are no longer required.
- VPN passwords must be changed on defined regular intervals as determined by the Information Technology Department.
- Only VPN clients approved by the Information Technology Department may be used.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Anti-Malware Policy

POLICY #: S2.14

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

Malware consists of viruses, spyware and other applications that are a risk to the security of WCMSCHF network and data resources. This policy provides guidance in safeguarding these resources from malware.

Scope:

WCMSCHF utilizes protective software and systems to reduce the risk of malware, such as viruses and spyware, from entering their systems or network. Risks of malware grow each month and properly functioning protection is critical to the safety and integrity of our network environment. This policy explains that WCMSCHF does take steps to minimize these risks and how you can support our efforts.

Policy:

Issuing Policy:

- All WCMSCHF computer systems will have anti-malware protection software installed as approved by the Information Technology Department.
- Employees will not override or negate the malware protections utilized by WCMSCHF.
- Employees will not install malware protections of their own or those that "pop-up" during internet activities.
- Employees will notify the Information Technology Department in the event that suspicious activity occurs on their system.
- Employees will be protective of their WCMSCHF resources and work in such a way as to minimize the threat of malware attack by accessing only respectable websites, work related websites, and being mindful of email threats.
- Employees will immediately notify the Information Technology Department if any of the following should occur:

- A message states that antivirus or antispyware protection has been disabled
- A messages states that your computer has a virus or spyware threat
- A message states that your antivirus or antispyware has not been properly updated
- You suspect a device is infected by malware or that you may have opened a link or attachment containing malware.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:

Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Removable Media Policy

POLICY #: S2.15

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.310(d)

NCQA STANDARD: B.2, B.3, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:

This document describes the requirements and appropriate use of removable media for WCMSCHF to minimize the risk of data loss or exposure of sensitive information maintained by WCMSCHF, and to reduce the risk of acquiring malware infections on computers operated by WCMSCHF.

Synopsis:

Removable media such as USB memory sticks are a significant risk to WCMSCHF and our network resources. They can store viruses that can be introduced to our network, and if not properly secured can risk the loss of PHI. WCMSCHF greatly limits the use of these types of devices, but this policy explains what is required in the few occasions where such a device would be useful.

Policy:

General Requirements

These requirements must be adhered to by individuals accessing WCMSCHF data, or data of entities affiliated with WCMSCHF on portable or removable media.

- Personal removable media devices, not supplied and managed by WCMSCHF, are strictly forbidden by WCMSCHF and will not be used on any WCMSCHF device nor contain WCMSCHF data or data of individuals or entities affiliated with WCMSCHF.
- IronKey and similar encrypted removable media devices will be provided to Employees by the Information Technology Department upon request and with sufficient cause.
- Encrypted information stored on removable media may be shared with appropriate entities within the business function of WCMSCHF to the extent otherwise permitted by WCMSCHF policies and procedures, if a password to decrypt the data is provided to the individual or entity separate from the removable media itself.

- The use of removable media should be limited to an as needed basis, and loss of removable media should be reported immediately to the Information Technology Department.
- The Information Technology Department will maintain a record of all WCMSCHF removable media devices, the Employee who checks out the device, and the reason necessitating the Employee's use of the device, the location and movement of the device, the date the Employee returns the device to the Information Technology Department, and the method used to wipe or dispose of the device.
- When a WCMSCHF removable media device is no longer required or is being reassigned it should be wiped clean of all data by the Information Technology Department before redistribution or storage, utilizing a Department of Defense DOD 5220.22-M overwrite procedure.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

- Acceptable Encryption Policy

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Intranet Policy

POLICY #: S2.16

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to specify those individuals that are allowed to submit updates to Internet facing sites as well as the Intranet, and the individuals responsible for ensuring that the updates are posted and restricted as necessary.

Synopsis:
This policy explains who is allowed to request information to be posted on our Intranet page and that the Information Technology Department is responsible for the act of posting and removing information from the Intranet.

Policy:

General

- The Information Technology Department will be responsible for the posting of information to Internet/Intranet sites, and to ensure its security as requested by management.
- After posting any updates, the Information Technology Department will notify the manager submitting the request and ask that the manager verifies that the update is working as desired.
- Only managers and approved Employees can submit changes to the Internet/Intranet sites, and only for the areas that they manage.
- Managers can request information be added and removed from the Internet/Intranet sites. However, they must submit the changes in a new document to the Information Technology Department. The Information Technology Department will not be responsible for updating content within a document.
- Documents should be submitted as PDF files when appropriate.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:
Created: June 22, 2010, by Hazen Weber
Approved: June 22, 2010, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Social Engineering Policy

POLICY #: S2.17

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(4)(ii)(B)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy is developed to make Employees aware of the threat of social engineering, how social engineering presents itself, and who to contact if Employees feel they have been compromised by social engineering.

Synopsis:
Social engineering often comes by way of manipulating personality traits, or working to gain confidence from individuals, so that they feel comfortable sharing information. Instances would be, holding a door for a person. This is polite but could allow someone access to a restricted area. Gaining trust could be by including enough information about a situation to seem authentic, but in all actuality they are "phishing" for additional information that may compromise the confidentiality of the patient and/or the organization.

Policy:

- Employees will not release information of a technical matter, such as specifics regarding software, computer and network hardware, or security practices, to individuals outside of WCMSCHF without prior approval from the Information Technology Department.
- Sensitive information such as passwords, models, serial number, or brand of resources, will not be shared to individuals outside of the organization.
- Employees will not share PHI or sensitive information unless the identity and authority of the recipient have been verified in accordance with the Privacy Master Policy P1.1 (Verification Requirements).
- Employees will not share information about WCMSCHF with reporters or the press, but instead will defer questions from reporters and the press to the Privacy and Security Officers.
- Employees will be aware of emotional language and actions designed to elicit a response by an unknown individual or entity such as "urgent matter," "virus emergency," "upper

management," name dropping, or using seductive comments and compliments about Employees' capabilities and intelligence, or rewarding Employees with gifts.

- Employees will not grant individuals unauthorized access to their devices or open emails that are part of a phishing or spear-phishing attack.
- Employees will ensure that access to a secured area is limited to them, and not hold the door, or open the door for unauthorized individuals.
- If Employees feel that they may have been manipulated into providing sensitive information or PHI to unauthorized individuals, they should immediately contact the Privacy and Security Officers by phone.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:
Created: July 18, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Patch Management Policy

POLICY #: S2.18

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(8)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

This policy states the expectation WCMSCHF has of Employees in helping to keep their computers systems safe and secure by use of software updates and patches, as well the expectations of the Information Technology Department to support and monitor the patch status of devices.

Synopsis:

Software, namely Microsoft Windows operating systems and Microsoft Office products, may have security vulnerabilities that are detected after they have been released to the public. To combat these vulnerabilities, Microsoft and other similar vendors, release updates to fill those gaps. This policy discusses what the Information Technology Department does to help fill these vulnerabilities by applying patches, and what Employees can do to help with this need.

Policy:

- The Information Technology Department will monitor workstation patches on a regular basis, as defined in a Standard Operating Procedure.
- The Information Technology Department will monitor server patch levels on a regular basis, as defined in a Standard Operating Procedure.
- The Information Technology Department will apply service pack updates on a regular basis, as defined in a Standard Operating Procedure.
- Information regarding patch updates will be stored in an Information Technology Change Control system or document.
- The Information Technology Department will monitor the firmware levels of core network components every six months and will apply updates as appropriate.
- The Information Technology Department will update home office routers and network hardware on an as needed basis.

- Employees will allow Microsoft Windows and Microsoft Office updates to run on their machine without interruption.
- Employees will apply Microsoft hot-fixes and patches when alerted by the Microsoft Update application.
- Employees should not update any applications aside from Microsoft products via the Microsoft Update application, without first seeking Information Technology Department approval.
- Employees will conform to the requests of patch management tools utilized by the Information Technology Department.
- The Information Technology Department will monitor and maintain, either by administrative or technical controls, the patching of third party products.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:
Created: July 18, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Periodic Evaluation of Standards

POLICY #: S2.19

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: July 28, 2014

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(8)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

The purpose of this Periodic Evaluation of Standards Policy is to set forth the requirements for WCMSCHF to conduct a technical and non-technical evaluation of the standards implemented to comply with the HIPAA Security Rule to ensure WCMSCHF's continued compliance with the HIPAA Security Rule. The periodic evaluation will also address whether environmental or operational changes necessitate updating WCMSCHF's Policies and Procedures.

Policy:

- The Security Officer will conduct an annual technical and nontechnical evaluation of WCMSCHF's security safeguards to determine whether WCMSCHF's Security Policies and Procedures meet the requirements of the HIPAA Security Rule. Evaluations will be conducted more frequently as needed based on changes the HIPAA Security Rule, changes to the organization of WCMSCHF, the availability or implementation of new technology, or security incidents.
- Security Incidents, newly acquired threats, and advancements in technology will also trigger more frequent evaluations to be conducted as needed.
- WCMSCHF evaluations will be conducted by the Information Technology Department.
- The evaluation will address whether WCMSCHF's Security Policies and Procedures are reasonable and appropriate to protect EPHI, and will evaluate whether additional HIPAA Security Rule addressable implementation specifications should be implemented.
- The evaluation will include, but is not limited to, a review of recent security incidents, risk assessments, and all other documentation retained pursuant to these Policies and Procedures during the applicable evaluation period.
- Employees are expected to cooperate fully with any evaluation being conducted.
- Employees are further expected to work with the Security Officer and the Information Technology Department in the development of a remediation plan, if applicable.

- Evaluations of WCMSCHF’s Security Policies and Procedures will be documented in writing and maintained in accordance with these Policies and Procedures.
- All evaluations will be submitted to the Executive Director along with recommendations for revisions to WCMSCHF’s security safeguards and these Policies and Procedures.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:
Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19 2016, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Business Associate Agreements

POLICY #: S2.20

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 6, 2013

RULES ADDRESSED: 45 C.F.R. § 164.308(b); 45 C.F.R. § 164.314

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

The purpose of this Business Associate Agreements Policy is to ensure that WCMSCHF obtains satisfactory assurances that any subcontractor that creates, receives, transmits, or maintains EPHI on behalf of WCMSCHF will appropriately safeguard the information. WCMSCHF will obtain satisfactory assurances through a written Business Associate Agreement.

Policy:

- Employees may not create, receive, transmit, or maintain EPHI unless a written Business Associate Agreement has been executed between WCMSCHF and the respective Covered Entity or Business Associate.
- WCMSCHF will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of a Covered Entity or Business Associate in accordance with the applicable Business Associate Agreement and HIPAA Security Rule.
- WCMSCHF may use and disclose PHI only as permitted by its Business Associate Agreements with Covered Entities or Business Associates, the HIPAA Privacy and Security Rules, the HIPAA Privacy and Breach Notification Policies and Procedures, and these Policies and Procedures.
- In accordance with 45 C.F.R. § 164.308(b)(2), WCMSCHF will ensure that any subcontractors that create, receive, maintain, or transmit EPHI on behalf of WCMSCHF agree to the same restrictions, conditions, and requirements that apply to WCMSCHF with respect to such information.
- The policies and procedures for entering into a Business Associate Agreement are governed by the Business Associate Agreements/Sub-Business Associate Agreements Policy (P1.3) and the Privacy Master Policy (P1.1).

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:
Business Associate Agreements/Sub-Business Associate Agreements Policy (P1.3)
Privacy Master Policy (P1.1).

Revision History:
Created: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19 2016, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Disposal of PHI Policy

POLICY #: S2.21

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: July 28, 2014

RULES ADDRESSED: 45 C.F.R. § 164.310(d)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this Disposal of PHI Policy is to address how WCMSCHF will destroy or dispose of PHI.

Policy:
<u>Disposal of PHI - Generally</u>
All PHI in paper, electronic or other format will be destroyed using an acceptable method of destruction after the appropriate document retention period has been met. Access to PHI stored on computer equipment and media will be limited by taking appropriate measures to destroy electronically stored PHI.

PHI must be destroyed or disposed of in accordance with the HIPAA Privacy Rule, HIPAA Security Rule, these Policies and Procedures and the HIPAA Security Policies and Procedures. *Employees must adhere to WCMSCHF's Privacy/Security Documentation Policy (P1.16/S4.3) when destroying or disposing of PHI.*

Employees may not destroy or dispose of records involved in a government investigation, public records request, audit, or litigation, or records that are required to be maintained by these Policies and Procedures or federal, state or local laws or regulations.

PHI must be destroyed or disposed of in a manner that renders the PHI unreadable, indecipherable, and prevents the PHI from being reconstructed. Methods may include shredding, burning, pulping, pulverizing, or other comparable methods. PHI should be stored and maintained in a secure location until the PHI is properly disposed of or destroyed. *Employees shall NOT abandon PHI or dispose of it in dumpsters, wastebaskets, recycling bins, or other containers that are accessible by the public or other unauthorized persons.*

If WCMSCHF uses a third party to destroy or dispose of PHI, WCMSCHF will enter into a Business Associate Agreement with the third party in accordance with these Policies and Procedures and the due diligence standards set forth in Section 75-64 of the North Carolina Identity Theft Protection Act. WCMSCHF will require the third party to promptly destroy the PHI in accordance with these Policies and Procedures and applicable law, including HIPAA and Section 75-64 of the North Carolina Identity Theft Protection Act. WCMSCHF will require such third party to provide proof of disposal or destruction of the PHI, including the methods used to destroy the PHI.

Hardware and Electronic Media

The destruction, disposal or reuse of hardware or electronic media containing PHI must be approved in advance by the Security Officer. The Security Officer will ensure that PHI is properly removed from all hardware and electronic media prior to the destruction, disposal or reuse of the device. Employees should consult with the Security Officer prior to the disposal of any hardware or electronic media, including without limitation any copier, printer, or fax machine (including before returning the device to the vendor or moving the device to a location that is accessible to unauthorized persons). The Security Officer will maintain a log of the movement and destruction of PHI from hardware and electronic media that may contain PHI.

See the IT Physical Asset Policy (S2.3) and the Fax and Copier Security Policy (S5.6) in the HIPAA Security Policies and Procedures for more information about the disposal, destruction, and reuse of electronic media and hardware that contains PHI.

Documentation of Destruction of PHI

The destruction of original records that contain PHI must be documented, including the date of destruction or disposal, the method of destruction or disposal, a description of the record, the dates covered by the record, the reason for disposal or destruction (such as in the normal course of business), and who destroyed or disposed of the record. Such documentation will be maintained in accordance with the Privacy/Security Documentation Policy (S4.3/P1.16).

Sanctions:

Individuals found violating these policies will be subject to appropriate sanctions in accordance with the Sanctions Policy (P1.15/S4.2).

Revision History:

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Data Protection Policy

POLICY #: S2.22

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED:

NCQA STANDARD: CM9 E3, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to ensure the protection of sensitive company information and PHI by requiring all Employees to participate in mandatory training and to sign a Confidentiality Agreement as required.

Synopsis:
WCMSCHF data is very sensitive and must be treated with utmost care. WCMSCHF requires training for all Employees regarding privacy and security policies at the start of employment and additional training at a minimum of once per calendar year. Each new employee must sign a Confidentiality Agreement. In this way, WCMSCHF hopes to build a culture that is mindful of the sensitive and confidential information we handle.

Policy:

- All new Employees must sign a Confidentiality Agreement. Employee Confidentiality Agreements are filed and reviewed monthly to verify they have been executed. A current version of the Confidentiality Agreement is maintained by the Privacy and Security Officers.
- Contractors, vendors and external parties approved to access WCMSCHF must sign a Visitor Confidentiality Agreement prior to accessing WCMSCHF systems. A current version of the Visitor Confidentiality Agreement is located on the Intranet under the Privacy and Security section.
- If the contractor, vendor, or external party will have access to EPHI, the party must sign a Business Associate Agreement prior to receiving access to the EPHI or WCMSCHF's systems.
- Confidentiality Agreements signed by internal Employees will be maintained and filed by the Security and Privacy Officers.
- Confidentiality Agreements signed by contractors, vendors and external parties will be filed by the Security and Privacy Officers at WCMSCHF and a copy will be provided to the vendor.

- All Employees accessing WCMSCHF systems will undergo privacy and security training within 30 days of their start time and will attend privacy and security awareness training yearly.
- Documentation of Employees attendance as privacy and security training and the yearly review of policies will be maintained by the Security and Privacy Officers.
- [1]Employees will treat all information stored, handled, and accessed by WCMSCHF as confidential.
- Employees will treat all PHI stored, handled, and accessed by WCMSCHF in compliance with Privacy and Security Policies and Procedures maintained by WCMSCHF, in compliance with applicable Business Associate Agreements, and in accordance with local, state and federal law.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:
Created: July 18, 2012, by Smith Anderson and Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Clean Desk Policy

POLICY #: S2.23

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 6, 2013

RULES ADDRESSED: 45 C.F.R. § 164.514(d)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The Clean Desk Policy explains the placement of confidential information to reduce the threat of a privacy incident or breach.

Synopsis:
We have a responsibility to both our patients and those we have entered into agreements with to ensure that their information is protected. Maintaining a clean desk by keeping sensitive and confidential information out of the view of others helps to fulfill these obligations.

Policy:

- Sensitive documents and PHI should be placed in locked drawer or cabinet before leaving the workspace.
- Sensitive information and PHI in paper format that is no longer in use should either be securely stored or disposed of via approved means.
- Sensitive information and PHI that is located on your computer screen or desk should be concealed from others in your office space who are not authorized to view or access such information.
- All workstations located in public areas must have a privacy shield installed.
- Workstations located in office spaces should be placed, if at all possible, in a way where the screen isn't in view of passersby.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Documents

- P1.1 (Privacy Master Policy)
- S2.3 (IT Physical Asset Policy)

Revision History:
Created: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Periodic Updates to Policies and Procedures

POLICY #: S2.24

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.530(i); 164.316

NCQA STANDARD: D.1, D.2, F.3

POLICY AUTHOR(S): Hazen Weber

WCMSCHF's Privacy and Security Policies and Procedures with respect to PHI are reasonably designed to comply with the standards, implementation specifications, and other requirements of the HIPAA Privacy Rule and HIPAA Security Rule applicable to Business Associates.

WCMSCHF acknowledges that certain requirements of HIPAA will be clarified in further guidance from the Secretary, and WCMSCHF agrees to revise these Policies and Procedures and its Business Associate Agreements as required by any guidance issued by the Secretary.

WCMSCHF will review these Policies and Procedures at least annually and will modify its Policies and Procedures (and corresponding policies in other HIPAA documents) as necessary to comply with changes in law, including, without limitation, changes to the HIPAA Privacy Rule and the HIPAA Security Rule. These changes must be promptly documented and implemented.

Sanctions:
Individuals found violating these policies will be subject to appropriate sanctions in accordance with the Sanctions Policy (P1.15/S4.2).

Revision History:
Effective: June 22, 2010, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: EPHI Transmission Policy

POLICY #: S3.1

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. §§ 164.312(a)(2)(iv); 164.312(e**)**

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

In compliance with the security controls specified under HIPAA, WCMSCHF shall implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

Synopsis:

This policy specifies how EPHI will be protected when it is in transmission.

Policy:

- WCMSCHF will protect EPHI sent from remote laptop and desktop clients to the WCMSCHF main network using industry standard safeguards.
- Employees will not send EPHI outside of the WCMSCHF network without encryption at such encryption levels specified by the Security Officer.
- WCMSCHF will require user authentication (both sending and receiving party) for any secure transmission of EPHI to and from network resources
- WCMSCHF will instruct Employees on appropriate means to transmit EPHI to and from non-WCMSCHF maintained resources and networks.

Procedures:

- WCMSCHF provides each remote laptop and desktop client with VPN software, which is used to establish an encrypted connection to the main network and requires authentication by the user.
- Email access within the main office is protected by a closed network and Exchange/Outlook communications are encrypted.
- Email access via the Outlook WebAccess interface (https://mail.wakedocs.org/owa) is encrypted using industry standard encryption practices.

- Email communications between the email server and WCMSCHF iPhones is encrypted, and the device itself is encrypted.
- Approved external systems utilized by Employees are protected and authentication is managed by the entity housing the information and in compliance with any agreements signed with WCMSCHF, including applicable Business Associate Agreements.
- Employees must consult with the Security Officer to obtain approval before transmitting WCMSCHF information, including PHI, to a service provider or external system not already approved by the Security Officer.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

- Virtual Private Network Policy
- Removable Media Policy
- Acceptable Encryption Policy
- Email an Email Retention Policy

Revision History:
Created: July 18, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Security Incident Reporting

POLICY #: S3.2

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(6)(ii)

NCQA STANDARD: C.3, F.3

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to establish procedures relating to security incident response.

Synopsis:
In the event that a security incident or a suspected security incident occurs, the Security Officer needs to be notified as certain steps, by law, must occur. This policy governs the response of both Employees and the Security Officer to a security incident.

Policy:

- Employees will report any actual or suspected security incident to the Security Officer immediately, by *phone* and *e-mail to the extent e-mail remains secure*. If you think the e-mail system is compromised by the suspected security incident, do *not* use e-mail to report the incident to the Security Officer. Please use the phone instead. A “security incident” is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- If the reported event is deemed to be a security incident, the Security Officer will work with witnesses and their managers in completing a security incident report**.** The Security Officer will document all security incidents and their outcomes in accordance with these Policies and Procedures.
- If Information Technology Department staff should witness unauthorized access on network systems that staff member should take action to immediately terminate the intruder’s access and to immediately report the incident to the Security Officer.
- WCMSCHF will take steps to mitigate any harmful effects of security incidents known to WCMSCHF, to the extent practicable. These steps should include the following:
    - Compromised systems must be removed from the network until the extent of the damage can be determined, and the threat is mitigated.

  - If the threat remains for the network, immediate action should be taken to mitigate the risk to other devices on the network.
- The Information Technology Department should make every effort to secure log and system files that could be used as evidence of a security incident, such as:
  - Backing up the affected environment.
  - Documenting all activities performed on the affected system or environment to contain, mitigate and restore the system or environment.
  - Storing any potential evidence, such as hard drives, in a secure environment.
  - Documenting and controlling the movement and handling of potential evidence in order to maintain a chain of custody.

  The Security Officer will serve as the coordinator and owner of all handling practices and processes in order to maintain a chain of custody.
- The Security Officer will notify senior management if mission critical systems or components will be made unavailable during inspection, processing and restoration.
- Any public release of information concerning a security incident must be approved by both the Security Officer and the Executive Director.
- The Security Officer, in consultation with the Privacy Officer, will notify applicable Covered Entities and other appropriate parties of the security incident, in accordance with the Business Associate Agreements with such Covered Entities.
- If a law enforcement official states to WCMSCHF that a notification required hereunder would impede a criminal investigation or cause damage to national security, WCMSCHF will:
  - If the statement is in writing and specifies the time for which a delay is required, delay such notification for the time period specified by the official; or
  - If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is submitted during that time.
- In the event of a security incident, no Employees outside of the Security Officer and the Executive Director or those authorized by the Executive Director, may make public comment regarding the incident, and Employees should direct all public inquiries to the Security Officer.
- Supervisors should take steps to mitigate security incidents by limiting employees’ access only to information needed to perform their job functions. The Security Officer will maintain a repository of security incident information for the purpose of analysis to determine if trends exist that could be mitigated through training, policy or technical controls.
- The Security Officer will conduct and document a post-incident analysis of any security incident and WCMSCHF’s response to determine if the Policies and Procedures could be improved to prevent or mitigate a similar security incident from occurring in the future or improve WCMSCHF’s response. The Security Officer will consider these findings in determining whether to update the Policies and Procedures.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:

Related Documents:

Revision History:

Created: July 18, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: May 21, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Privacy and Breach Notification/Security Joint Policy

POLICY TITLE: Training and Awareness

POLICY #: P1.14/S4.1

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.530(b); 164.308(a)(5)

NCQA STANDARD: D.1, E.1, E.2, E3, F.3

POLICY AUTHOR(S): Tara Kinard, Hazen Weber

Purpose:
This Training and Awareness Policy sets requirements in frequency and content for privacy and security awareness training for Employees.

Synopsis:
Privacy and Security laws governing our organization change and these changes impact WCMSCHF, Employees and the patients and entities to which we have obligations. The Privacy and Security Officers must notify staff of these changes and provide supporting information via policies and procedure documents. This policy explains the ways by which Employees will be made aware of our current privacy and security policies, how we provide regular training and how Employees will be updated with changes.

Policy:

- Each new Employee will receive privacy and security training as specified by the orientation schedule, usually within the first week, but no later than 30 days after the start of employment.
- Each new Employee will be required to read all WCMSCHF privacy and security policies and sign an acknowledgement form stating that they have done so.
- Each new Employee will be required to enter into a Worker Confidentiality, Non-Disclosure, and Non Solicitation Agreement with WCMSCHF, agreeing to comply with the WCMSCHF privacy and security policies and to protect the confidentiality of sensitive information, including PHI. A current version of the Agreement is maintained by the Privacy and Security Officers.
- All signature forms will be stored for a period of at least six years.
- The Privacy and Security Officers will hold at least one awareness presentation each calendar year that is mandatory for all Employees to attend. The awareness training

will contain highlights of policies and Standard Operating Procedures, changes to policies and Standard Operating Procedures and examples of lessons learned.

- All Employees will be required to review and sign an acknowledgement form stating that they have re-read all privacy and security policies once each year, in coordination with the annual awareness training.
- When WCMSCHF makes a material change to these Policies and Procedures, it will provide additional training for those Employees affected by the change within 30 days of such change.
- Employees who violate privacy and/or security policies may be asked to attend an awareness training for new hires or a one-on-one awareness training at the discretion of their manager or the Privacy and/or Security Officers and per the Sanctions Policy (P1.15/S4.2).

Revision History:
Effective: June 22, 2010, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Privacy and Breach Notification/Security Joint Policy

POLICY TITLE: Sanctions

POLICY #: P1.15/S4.2

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. § 164.530(e); 164.308(a)(1)(ii)(C)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Tara Kinard, Hazen Weber

Purpose:
This Sanctions Policy specifies what considerations and actions can be taken in the event that sanctions are levied against an employee for violating a privacy and/or security related policy. This policy is a mandatory requirement of HIPAA.

Synopsis:
Sanctions are a necessary part of business and a requirement by law. This policy explains some of the variables and considerations that will be taken into account when applying a specific sanction, so that the process is as transparent as is reasonably possible. It also serves as a guide to senior management so that violations with like circumstances will be met with like sanctions and are thus fair.

Policy:
Sanctions will be levied against Employees who violate any security and/or privacy policy by use of defined categories for incident types as specified below.

> *Category 1:*
> Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge or judgment (e.g., emailing PHI to an employee's personal email account).
>
> *Category 2:*
> Deliberate unauthorized access to PHI, without loss or Disclosure (e.g., Employee accessing confidential information of a co-worker without a legitimate business reason or sharing a password with a co-worker).
>
> *Category 3:*

Deliberate unauthorized access of PHI or deliberate tampering of data but done without malice or personal gain (e.g., staff accessing information and Disclosing to an unauthorized individual or tampering with an electronic document to expedite a process).

Category 4:
Deliberate unauthorized Disclosure of PHI for malice or personal gain (e.g., selling information to the tabloids or using personal information to open lines of credit).

Before sanctions will be levied, consideration will be given to the following mitigating factors:

- Offending Employee voluntarily admits the breach and cooperates with the investigation;
- Offending Employee shows remorse;
- Action was taken under pressure from an individual in a position of authority;
- Employee was inadequately trained;
- Offending Employee has multiple offenses;
- Whether or not harm came to the breach victim(s);
- Type of breach (e.g., specially protected information such as HIV-related, psychiatric, substance abuse and genetic data):
    - High volume of people or data affected
    - High exposure for the institution and marked damage to the Company's reputation
    - Large organizational expense incurred, such as breach notifications
    - Hampering an investigation
    - Negative influence of actions on others

Sanctions specified within this document are for privacy and security violations and fall outside of those specified within the Employee Handbook.

Sanctions have been specified below as general guidelines and are dependent on the circumstances of the violation.

Types of Sanctions:

- A written sanction specifying the incident and the appropriate process that should have been followed will be sent to the Employee and his or her direct supervisor by either the Privacy and/or Security Officer and will be signed and filed along with an entry in the Incident Log, which shall be maintained by the Privacy Officer and Security Officer for at least six years.
- A written sanction as described in #1 and a mandatory one-on-one training with the Privacy and/or Security Officer.
- A written sanction and a mandatory one-on-one training as described in #2 along with a written warning will be filed in the employee's personnel file for a period of two years.
- A written sanction and mandatory one-on-one training as described in #2 along with a final written warning will be filed in the employee's personnel file for a period of one year.
- Other sanctions include demotion, loss in pay, leave without pay and termination of employment.

Revision History:

Effective: June 22, 2010, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Privacy and Breach Notification/Security Joint Policy

POLICY TITLE: Privacy/Security Documentation

POLICY #: P1.16/S4.3

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: June 22, 2010

RULES ADDRESSED: 45 C.F.R. §§ 164.530(j); 164.316

NCQA STANDARD: A.3

POLICY AUTHOR(S): Tara Kinard, Hazen Weber

WCMSCHF shall maintain these Policies and Procedures in written or electronic form. It shall also maintain, in writing or in electronic form, any communication required to be in writing by these Policies and Procedures. Also, if any action, activity or designation is required by these Policies and Procedures to be documented, WCMSCHF shall maintain a written or electronic record of such action, activity or designation.

WCMSCHF will retain all documentation noted above for at least six years from the date of its creation or the date when it last was in effect, whichever is later. Information no longer required to be retained by these Policies and Procedures (including this Privacy/Security Documentation Policy) will be destroyed by secure means. Any and all documentation that becomes part of a medical record will be retained according to the laws applicable to retention of medical records.

Employees may not destroy or dispose of records involved in a government investigation, public records request, audit or litigation or records that are required to be maintained by these Policies and Procedures or federal, state or local laws or regulations.

All PHI must be destroyed or disposed of in accordance with the Disposal of PHI Policy (S2.21).

WCMSCHF has also implemented Financial Policies and Procedures for the retention and destruction of certain financial documents of WCMSCHF that supplement, but do not replace, the document retention requirements described in this Policy.

Revision History:
Effective: June 22, 2010, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: August 21, 2013, by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Risk Assessment Policy

POLICY #: S5.1

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: C.F.R. § 164.308(a)(1)(ii)(A)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

This Risk Assessment Policy is designed to empower the Security Officer and the Information Technology Department to perform periodic security risk assessments (RAs) for the purpose determining areas of potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by WCMSCHF, and to initiate appropriate remediation.

Scope:

Risk assessments can be conducted on any entity within WCMSCHF. RAs can be conducted on any physical asset or information system including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy:

- The execution, development and implementation of remediation programs are the joint responsibility of the Security Officer with the help of the Information Technology Department and the department responsible for the information system or physical asset being assessed
- The Security Officer, in consultation with the Information Technology Department, will document and maintain detailed written procedures for conducing risk assessments, including the criteria for evaluating potential risks and vulnerabilities of EPHI and a plan to ensure all systems that contain, process, or transmit EPHI are regularly assessed.
- Employees are expected to cooperate fully with any RAs being conducted on physical assets and information systems for which they are held accountable.
- Employees are further expected to work with the Security Officer and the Information Technology Department Risk Assessment Team in the development of a remediation plan.

- RA’s will be conducted during the implementation of new hardware or network services.
- The Security Officer, in coordination with the Information Technology Department will conduct a yearly risk assessment of WCMSCHF unless concerns warrant more frequent review. The Security Officer will update the procedures for risk assessments as the Security Officer determines is advisable based on changes in WCMSCHF’s environment.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Related Documentation:

- Business Impact Analysis Document

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Vulnerability Assessment Policy

POLICY #: S5.2

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: C.F.R. § 164.312(b)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

The purpose of this policy is to specify the handling of vulnerability assessments both internally by Employees and through the assistance of external contracted support. The vulnerability assessment will on be conducted with the approval and in conjunction with the Information Technology Department.

Vulnerability assessments may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents to ensure conformance to WCMSCHF security policies
- Monitor user or system activity where appropriate.

Scope:

This policy covers all computer and communication devices owned or operated by WCMSCHF and Personal Communication Devices used to access WCMSCHF data resources. This policy also covers any computer and communications device that are present on WCMSCHF premises which are or have been connected to WCMSCHF's systems or network, even if not owned or operated by the WCMSCHF.

Policy:

WCMSCHF reserves the right to monitor and audit all WCMSCHF system activity and equipment, Electronic Media, and Personal Communication Devices used to access WCMSCHF data resources in accordance with these Policies and Procedures, including this Vulnerability Assessment Policy.

The Security Officer and the Information Technology Department will work together to develop, implement, and document appropriate policies, procedures, and protocols that set forth the hardware, software, and procedural mechanisms to audit the information systems that contain EPHI. A record of these measures will be documented and maintained by the Security Officer.

WCMSCHF (through the Security Officer) may allow approved contract organizations and the Information Technology Department to perform the assessments authorized in this policy. WCMSCHF shall provide protocols, addressing information, and network connections sufficient for the assessments with approved software.

This access may include:

- User level and/or system level access to any computing communications device.
- Access to information (electronic, hardcopy, etc.) that may be created, received, transmitted, or maintained on WCMSCHF equipment or premises.
- Access to work areas (offices, server closets).
- Access to interactively monitor and log traffic on WCMSCHF networks.

The Information Technology Department will be responsible for contacting any necessary vendors that may be impacted by vulnerability assessments and will notify management and employees of any impact to network stability or speed. Management and impacted vendors will be notified in writing what systems are being tested, the time frame of the assessment, and who to contact with questions or concerns during the assessment.

The Security Officer will annually oversee the review of WCMSCHF's systems and applications to determine whether upgrades to WCMSCHF's assessment capabilities are needed. WCMSCHF will document these findings in accordance with these Policies and Procedures.

Please see the Monitoring and Logging Policy (S5.4) for more information about WCMSCHF's ongoing monitoring and logging efforts.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Contingency Plan Policy

POLICY #: S5.3

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(7)(ii); 45 C.F.R. § 164.312(a)(2)(ii)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy serves to outline WCMSCHF's policies and procedures to safeguard the confidentiality, integrity, and availability of EPHI during an emergency or other occurrence that negatively impacts systems that contain EPHI. This Policy is based upon the control entitled, "Establish and maintain a systems continuity framework". The framework provides the overarching need for systems continuity. Therefore, it should be established and maintained at the highest level of the Information Technology Department organization.

Synopsis:
We are required to develop a means to safeguard the confidentiality, integrity, and availability of EPHI in the event of a catastrophe. This could be something relatively small such as a short-term power outage, larger such as a server hardware failure, or catastrophic such as a fire damaging our technology infrastructure. This policy creates a framework of how these situations will be handled and relies on the Disaster Recovery Plan for specific details regarding the handling of these types of situations. The Disaster Recovery Plan is maintained separately by the Security Officer and is available to Employees on an as needed basis. Please see the Security Officer for the current version of the Disaster Recovery Plan.

Policy:

- WCMSCHF will respond to emergencies or other incidents such as fire, vandalism, system failure, and natural disasters that may damage systems containing EPHI.
- WCMSCHF will create and maintain retrievable exact copies of EPHI in order to restore any loss of data.
- WCMSCHF will continue critical business processes for protection of the security of EPHI while operating in emergency mode.
- WCMSCHF will periodically test and evaluate contingency and emergency mode operations for their effectiveness, and make appropriate corrections.

- WCMSCHF will develop a Disaster Recovery Plan, and store the plan both onsite and remotely for safe and secure access in the event of a disaster.
- The Disaster Recovery Plan will be reviewed at a minimum yearly, but more frequently as changes to the network infrastructure and the value of certain systems change.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Monitoring and Logging Policy

POLICY #: S5.4

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.308(a)(1)(ii)(D); 164.312(b)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
This policy is based upon the control entitled, "Establish and maintain logging and monitoring operations", and is implemented to specify what monitoring and reporting the Information Technology Department will perform, and how and when the information will be reviewed.

Synopsis:
WCMSCHF is responsible for being able to audit the actions of users, and to utilize audit logs to determine security concerns and to take appropriate action based on those findings.

Policy:

- WCMSCHF shall identify and respond to suspected or known security incidents, mitigate to the extent practicable, and document the security incidents and their outcomes.
- WCMSCHF shall implement hardware, software and defined processes to record and examine user and system activities that involve EPHI, including audit logs. A record of these measures will be documented in writing by the Security Officer**.**
- WCMSCHF shall implement procedures to review audit logs, access reports, and security incidents and access to EPHI on a regular basis. These procedures will be documented in writing and maintained by the Security Officer in accordance with these Policies and Procedures.
- Where feasible, the systems will be configured to provide alerts based on predefined events. WCMSCHF will promptly investigate and respond as appropriate to all alerts.
- All Server Event and System logs, and reports associated with a security incident or a security breach shall be retained for a period of at least six years from date of occurrence in accordance with the Security/Privacy Documentation Policy (S4.3/P1.16). All other data shall be retained for a period of 90 days.

- Security incidents suspected or known, as they manifest will be reported immediately to the HIPAA Security Officer.
- Every security incident will be analyzed for its impact and possible remedial actions and will be documented.
- The Information Technology Department will review Server Event and Network Device System log information on a regular basis as defined in a Standard Operating Procedure, unless concerns warrant more frequent review.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Backup Policy

POLICY #: S5.5

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. §§ 164.308(a)(7)(ii); 164.310(d)(2)(iv)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of this policy is to safeguard the information resources of WCMSCHF by implementing technologies and processes that prevent the loss of EPHI in the case of accidental deletion, corruption or in the case of a disaster, and to ensure timely restoration of EPHI should such an event occur.

Synopsis:
WCMSCHF manages and houses a great deal of EPHI via files on our servers, databases, and email. Aside from the EPHI that Employees utilize on the system, there are also files like the operating system that allow these services and systems to function. WCMSCHF has implemented technologies that will work to keep EPHI and associated data, including software and operating system information, stored on these systems safe. This policy explains not only how we do that, but also explains that how you save our information will have an impact on whether it is backed up or not.

Policy:

- The Information Technology Department is responsible for configuring, maintaining, monitoring and executing data backups and restorations on supported server-side systems.
- Active use files will be backed up as defined within the Backup Standards document and stored off-site via a secured remote data vault solution utilizing industry standard encryption in both the transmission of information and in its storage.
- WCMSCHF will remain the owner of all encryption keys for all backup processes both remote and local.
- Archived information no longer in active use will have a single instance vaulted online and will be kept locally as well.
- An image level backup of the primary server systems will be run as specified by the Backup Standards document.

- Drives containing image level backups will be rotated offsite from their original location.
- All image level backups will be encrypted utilizing industry standard encryption.
- Restoration of files will be done if at all possible, in a way that will not overwrite existing files, even the file they are intended to replace.
- Twice a year, full image level restorations will be tested and documented.
- Twice a year, critical system files will be restored as a test and documented.
- The Information Technology Department will monitor backups for performance and completion.
- Requests for file restoration must be made to the Information Technology Department via the Information Technology Support email address.
- Media utilized for backup will be wiped following best practice upon retirement or disposal, in accordance with WCMSCHF's Disposal of PHI Policy (S2.21).

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:
DoD 5220.22M
Backup Standards Document

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28, 2015, by WCMSCHF Board of Directors

Revised: July 6, 2016, by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016, by WCMSCHF Board of Directors

Revised: July 3, 2017, by Smith Anderson and Hazen Weber
Approved: XXXXXX, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Fax and Copier Security Policy

POLICY #: S5.6

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § 164.310(d)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:
The purpose of the policy is to specify the appropriate handling of fax transmissions and disposal or recycling of fax and copier equipment with memory for information storage, which may have processed PHI.

Synopsis:
Devices that offer fax and copying or scanning capability often times contain data storage devices such as memory or a hard drive, that store information as it is being processed. If the data being handled is PHI, there is a possibility that PHI may remain accessible on the drive after it is processed. WCMSCHF needs to ensure that fax and multifunction devices leaving our organization do not have PHI stored on them.

Policy:

- Fax machines should be placed in low traffic private areas.
- Employees must retrieve faxes from the fax machine in a timely manner.
- All WCMSCHF faxing systems comply with the HIPAA Security Rule requirements and may be used to transmit documents containing PHI only if the transmission complies with WCMSCHF policies and procedures, the HIPAA Privacy and Breach Notification Policies and Procedures, and the applicable Business Associate Agreement.
- All faxes should contain a cover page detailing who the fax is for and who the sender is. If the fax contains confidential information, including PHI, the cover page should be marked as “Confidential”.
- Devices that offer fax, copy, scanning and print capabilities or any combination thereof must be approved by the Information Technology Department for disposal, recycling, or return to vendor.
- Devices that contain volatile memory only must be unplugged from power for a minimum of 5 minutes prior to disposal

- Devices that contain non-volatile storage such as hard drives or flash memory must be wiped utilizing best practices, or removed from the system and destroyed, prior to disposal.
- Documentation that these actions have taken place prior to the removal of the hardware must be filed by the Information Technology Department for all devices containing non-volatile storage.

Sanctions:
Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Standards:
7 Pass US DoD 5220 Method

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: FTP Connection Policy

POLICY #: S5.7

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 7, 2012

RULES ADDRESSED: 45 C.F.R. § §164.312(e)(2)

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose

This document describes requirements for FTP communication to WCMSCHF network resources.

Scope

This policy applies to all individuals or entities affiliated with WCMSCHF that will access WCMSCHF maintained data from a remote site utilizing FTP based communications with the consent of WCMSCHF.

Policy

Issuing Policy

FTP connections from external networks must be approved by the Information Technology Department prior to access to WCMSCHF data resources and must abide by the following requirements:

- FTP communications will only be approved with respect to individuals and entities that have a Business Associate Agreement with WCMSCHF and for the term and access approved by WCMSCHF management in accordance with the principle of "minimum necessary."
- FTP access to WCMSCHF data resources must be implemented and maintained by the Information Technology Department.
- FTP access will require the update of firewall restrictions to limit FTP protocol access only to the static external IP address of the individual or entity that has been approved for access.
- Access to the FTP server will be further restricted by requiring a username and a password that complies with the Password Policy.
- Each individual or entity will be granted access to their own designated directory from which data can be sent or received.

- FTP directories will be by default restricted to only allow data deposits, unless otherwise specified in writing.
- FTP communication will be encrypted as specified by the Encryption Standards Document.
- Access can be terminated at any time without cause by WCMSCHF.
- Access will be terminated upon the request of WCMSCHF management in the event that the connection is no longer required.

Sanctions:
Individuals found violating this policy will be subject to appropriate sanctions in accordance with the Sanctions Policy (S4.2/P1.15).

Revision History:
Created: September 6, 2012, by Hazen Weber
Approved: September 7, 2012, by Susan Davis

Revised: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors

Revised: May 20, 2015, by Smith Anderson and Hazen Weber
Approved: July 28th, 2015, by WCMSCHF Board of Directors

POLICY

Wake County Medical Society Community Health Foundation

POLICY TYPE: Security Policy

POLICY TITLE: Network Security Policy

POLICY #: S5.8

NEW, REVISED, RESCINDED: Revised

EFFECTIVE DATE: September 6, 2013

RULES ADDRESSED:

NCQA STANDARD: N/A

POLICY AUTHOR(S): Hazen Weber

Purpose:

The policy is intended to protect the integrity of the WCMSCHF network, and to mitigate threats that might impact the security and reliability as well as performance of the network. This policy is necessary to provide a reliable network for the continuity of business for WCMSCHF.

Synopsis:

Certain protections and procedures need to be in place to ensure that the network infrastructure is reliable and Employees are able to fulfill their work related obligations. This policy explains what some of the protections are.

Policy:

- The Information Technology Department is responsible for configuring and maintaining WCMSCHF network infrastructure and systems, providing users with systems access upon proper approval, maintaining network security measures and updating protections as necessary, monitoring WCMSCHF network for unauthorized activity and security incidents and responding to and mitigating such incidents should they occur.
- The Information Technology Department is responsible for maintaining the reservation of domain name spaces, including those registered for the use of a web presence.
- The Information Technology Department may delegate administrative responsibilities to individuals or organizations for certain specific duties so approved.
- The Information Technology Department will provide prior notice to Employees who may be impacted by network changes to the extent feasible.

- Employees are not authorized to connect or allow a vendor to connect any device to the WCMSCHF network or reconfigure or change any WCMSCHF network settings (including security settings or firewalls) without providing prior notice to the Information Technology Department and receiving prior approval from the Information Technology Department.
- Unauthorized access to network equipment is not permitted.
- Employees are not authorized to install or implement proxy servers on the WCMSCHF network.
- The Information Technology Department will investigate any unauthorized access to WCMSCHF systems.

Sanctions:

Individuals found violating this security policy will be subject to sanctioning in compliance with the Sanctions Policy (S4.2/P1.15).

Revision History:

Created: September 6, 2013, by Hazen Weber
Approved: September 6, 2013, by Susan Davis

Revised: June 20, 2014, by Smith Anderson and Hazen Weber
Approved: July 28, 2014, by WCMSCHF Board of Directors