WISHIN

Wisconsin Statewide Health Information Network

2012

System Security Policies

Contents

Introduction

This System Security document is intended to set forth the administrative, technical, and physical safeguards WISHIN has in place to protect the security and integrity of the confidential information that is part of the WISHIN Pulse health information exchange.

This document is not the actual contract between WISHIN and its HIE vendor. However, WISHIN asserts that policies within this document are consistent with the contractual safeguards agreed to between WISHIN and its contracted HIE vendor.

Common Terms and Definitions

The following terms are commonly used throughout this document, and their meanings should be interpreted as defined below, unless otherwise specified:

Confidential Information
All patient protected health information, employee information, business information, and proprietary information stored and/or accessed by WISHIN and/or its contracted HIE vendor.

WISHIN
The Wisconsin State Health Information Network, including all of its employees, Board members, committee members, and workgroup members.

WISHIN Contracted HIE Vendor
The software provider contracted with WISHIN to host the WISHIN Pulse health information exchange (HIE).

Participant
A facility/organization sending information to and/or receiving information from WISHIN Pulse. Types of participants may be, but are not limited to, hospitals, clinics, care facilities, payers, and Public Health.

User
A person who is authorized to use the WISHIN Pulse health information exchange. A user may be a person authorized to view a participant's version of WISHIN Pulse, a WISHIN workforce member, or a contractor authorized by WISHIN or a participant.

Workforce
Employees or contractors of WISHIN.

Policy 100: Information Stewardship

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor.

Policy

WISHIN and its contracted HIE vendor will protect the security and privacy of all Confidential Information entrusted to it.

Overview

WISHIN is committed to protecting the security and privacy of all information entrusted to it and its contracted HIE vendor. WISHIN's services and internal operating processes and procedures will be in compliance with laws and regulations, as well as established industry best practices.

The purpose of this policy and all related policies (the "Plan") is to provide a framework for protecting information. Information is no longer simply something which supports the provision of a product or service. Information itself has become an asset.

The purpose of this Plan is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the administrative, technical, and physical security of WISHIN technology resources.

An information security management policy is necessary to serve goals pertaining to operations, records, and facilities. These include:

- Ensuring continuity of operations
- Protecting the integrity of business records
- Preventing unauthorized access to records
- Protecting privacy and security of confidential information

The primary objectives of this Plan and its associated policies are:

- To effectively manage the risk of security exposure or compromise within the systems.
- To communicate the responsibilities for the protection of information.
- To establish a secure processing base and a stable processing environment.
- To promote understanding and compliance with all applicable laws and regulations.
- To protect management and preserve management's options in the event of an information asset misuse, loss, or unauthorized disclosure.

Responsibilities of WISHIN Management

In accordance with other company policies and procedures, WISHIN management is responsible for:

1. Establishing administrative, technical, and physical safeguards to protect the privacy and security of information.
2. Ensuring a sufficient level of training takes place for people entering or modifying data in the system.

3. Assisting with contingency planning efforts and categorizing information (or specific application systems) according to a criticality scale.
4. Making decisions about the permissible uses of information.
5. Understanding the uses and risks associated with information. This means they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they have responsibility.
6. Protecting the information in the possession of WISHIN and its contracted HIE vendor from unauthorized access, alteration, destruction, or usage.
7. Providing and administering general controls such as back-up and recovery systems consistent with company policies and standards.
8. Establishing, monitoring and operating information systems in a manner consistent with policies and standards.

Responsibilities of WISHIN Staff and Other Workers

In accordance with other company policies and procedures, employees, contractors, consultants, temporaries, other workers at WISHIN are responsible for:

1. Using the information only for the purposes specifically approved by management.
2. Complying with all WISHIN security measures.
3. Refraining from unauthorized access, use, and/or disclosure of information in their possession.
4. Reporting all incidents in which they believe a privacy or information security vulnerability or violation may exist.

Violation

Any member of the workforce found to have violated this Plan or its associated policies may be subject to disciplinary action, up to and including termination.

Reporting and Review

WISHIN will update and review the Plan as needed, but no less than every two years.

The WISHIN Security Officer will report significant privacy and security issues to the designated committees of the Board of Directors along with periodic updates regarding the Plan.

Policy 200: Privacy and Security Governance

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN's Board, and/or any committee it may designate, will provide oversight and guidance in establishing WISHIN's privacy and security policies.

Responsibilities

The Board or its designated committee(s) will be responsible for providing overall direction and management regarding privacy and security and this Plan. Specifically, it will ensure WISHIN:

1. Establishes privacy and security policies and practices.
2. Reviews and modifies privacy and security policies and practices in light of operating experience, changes in law, and changes in available compliance tools.
3. Establishes a privacy and security officer.
4. Maintains working relationships with legal counsel and outside consultants and uses the services of such parties to assist with its responsibilities.
5. Maintains working relationships with the privacy and security officers and managers of the institutions participating in WISHIN.
6. Represents a cross-section of the WISHIN participants.

Policy 300: Security Officer

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN will designate an individual to act as its Security Officer. The Security Officer will have authority commensurate with his or her responsibilities. The Security Officer will be responsible for the operational aspects of this Plan, in coordination with the WISHIN Chief Executive Officer, Chief Operations Officer, and the contracted HIE vendor.

Responsibilities

The Security Officer role is responsible for operational matters regarding security and the day-to-day execution of this Plan. Specifically, the role:

1. Reviews and recommends modification of this Plan and all supporting policies and procedures in light of operating experience, changes in HIPAA and any applicable state law, and changes in available compliance tools.
2. Exercises responsibility for the development and implementation of this Plan.
3. Is responsible for implementing, managing, and enforcing information security directives as mandated by WISHIN, this Plan, HIPAA, and applicable state and federal laws.
4. Ensures the ongoing integration of information security with business strategies and requirements.
5. Ensures the access control, disaster recovery, business continuity, incident response, and risk management needs of the organization are properly addressed.
6. Works with vendors, outside consultants, and other third parties to improve information security within the organization.
7. Performs ongoing information risk assessments and audits to ensure information systems are adequately protected in accordance with HIPAA requirements.
8. In conjunction with the Privacy Officer, leads privacy, confidentiality, and security awareness and training initiatives to educate the workforce and users about risks.
9. Directs and reviews the findings from risk assessments and audits of information systems and privacy and security practices.
10. Directs the incident response team to contain, investigate, and prevent future privacy and security breaches.
11. Monitors the effectiveness of this Plan and incorporates the results of monitoring into recommendations for amendment, sanction, or other action.
12. Assures timely and effective training and retraining of the workforce.
13. Uses judgment in assessing exposure, recommending solutions, and overseeing compliance with this Plan.

14. Maintains working relationships with legal counsel and outside consultants and uses the services of such parties to assist with implementing this Plan.
15. Maintains working relationships with the privacy and security officers and managers of the institutions participating in WISHIN.
16. Maintains working relationships with the privacy and security officers and managers of WISHIN's contracted HIE vendor.

Policy 400: Privacy Officer

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN will designate an individual to act as its Privacy Officer. The Privacy Officer will have authority commensurate with his or her responsibilities. The Privacy Officer will be responsible for the operational aspects of Privacy, in coordination with the WISHIN Chief Executive Officer, Chief Operations Officer, and the Policy Advisory Committee.

Responsibilities

The Privacy Officer is responsible for operational matters regarding the implementation of the Privacy Policies and related privacy matters. Specifically, the role:

1. Exercises responsibility for the development and implementation of the Privacy Policies.
2. Monitors changes to HIPAA and other existing state and federal privacy laws and analyzes new privacy regulations, for impact on WISHIN operations.
3. Reviews and recommends modification of the Privacy Policies and all supporting policies and procedures in light of operating experience, changes in HIPAA, or other applicable privacy laws, and changes in available compliance tools.
4. Is responsible for implementing, managing, and enforcing privacy directives as mandated by the Board's designated committees, the Privacy Policies, HIPAA, and applicable state and federal laws.
5. Documents and monitors WISHIN's relationship as a business associate to covered entities participating in WISHIN to ensure compliance with HIPAA and contractual requirements.
6. Ensures the ongoing integration of privacy protections with business strategies and requirements.
7. Participates in ongoing information risk assessments and audits to ensure privacy is adequately protected and meets HIPAA and state law requirements.
8. In conjunction with the Security Officer, leads privacy, confidentiality, and security awareness and training initiatives to educate the workforce and users about risks.
9. Works with vendors, outside consultants, and other third parties to improve privacy practices within the organization.
10. Participates on the incident response team to contain, investigate, mitigate, and prevent future privacy breaches.
11. Receives privacy complaints and responds to questions from participants and third parties regarding WISHIN's privacy practices.
12. Responds to requests by entities or individuals for access to information as appropriate to the situation.

13. Maintains a database of disclosures, requests, business associate agreements, and other privacy-related documentation.
14. Monitors the effectiveness of the Privacy Policies and incorporates the results of monitoring into recommendations for amendment, sanction, or other action.
15. Develops and implements sanctions as appropriate for issues of non-compliance.
16. Assures timely and effective training and retraining of the workforce.
17. Uses judgment in assessing exposure, recommending solutions, and overseeing compliance with the Privacy Policies.
18. Maintains working relationships with legal counsel and outside consultants and uses the services of such parties to assist with implementing the Privacy Policies.
19. Maintains working relationships with the privacy and security officers and managers of the institutions participating in WISHIN.
20. Maintains working relationships with the privacy and security officers and managers of WISHIN's contracted HIE vendor.

Policy 500: Risk Analysis and Management

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor.

Policy

WISHIN will work with its contracted HIE vendor to conduct an initial risk assessment and subsequent risk assessment(s), as appropriate, to identify the potential risks to and vulnerabilities of electronic Protected Health Information ("ePHI") possessed or maintained by WISHIN. WISHIN and its vendor will further adopt and implement reasonable and appropriate administrative, technical, and physical safeguards and security measures to protect against any reasonably foreseeable threats to the privacy, integrity, and availability of the ePHI and the information systems in which it is created, received, transmitted, and maintained.

Risk Assessment

WISHIN and its vendor will conduct security risk assessments periodically and whenever significant changes occur in the WISHIN information technology environment. The risk assessments will:

1. Comply with security audit guidelines set forth by NIST, ISO 27001, or similar protocols.
2. Be reviewed and accepted by the committee designated by the Board.
3. Identify the potential risks and vulnerabilities to the confidentiality, integrity, and availability of critical data and information technology.
4. Identify potential means to mitigate such risks and vulnerabilities.
5. Identify areas where WISHIN's Information Security Plan fails to satisfy the requirements of the HIPAA Security Rule and other applicable information security laws, statutes, and regulations.

Software Purchases, Upgrades, and Development

WISHIN's purchase of software, upgrades, and development relative to ePHI will take into account potential impact on applicable information security laws, statutes, and regulations, including HIPAA compliance. WISHIN will consider its Security Plan when evaluating hardware and software acquisitions and upgrades relative to ePHI.

Policy 600: Sanctions and Corrective Actions

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN will apply sanctions to workforce members who violate HIPAA Security and Privacy Compliance policies and procedures.

Examples of Sanctions

Examples of sanctions include, but are not limited to:

1. Verbal warnings
2. Written warnings
3. Employment suspension
4. Termination of access to Electronic Protected Health Information
5. Termination of employment

HIPAA Security Confidentiality Agreement

Workforce members will agree to comply with security policies and procedures and acknowledge this sanction policy by signing a confidentiality agreement.

Application of Sanctions

WISHIN will apply all sanctions to all workforce members consistent with existing personnel policies and procedures.

Policy 700: Information Systems Activity Review

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor.

Policy

WISHIN will review information systems activity on a periodic basis to determine whether Electronic Protected Health Information ("ePHI") is accessed, used, or disclosed inappropriately.

Examples of Information System Activity Records

Examples of information system activity records may include, but are not limited to, audit logs, access reports, and Security Incident reports.

Records Reviews

WISHIN will determine the records to be reviewed, the frequency of such review, and the individual responsible.

Security Incidents

Any Security Incidents identified as a result of information systems activity review will be investigated as outlined in the Security Incident Policy and Procedures.

Audits and Reports

WISHIN will:

1. Conduct random security audits
2. Conduct red flag reporting
3. Perform complaint-based investigation

WISHIN will report the findings from these review activities to the Security Officer and, as applicable, to the Privacy Officer for review and action. WISHIN will use aggregate findings from system security reviews for training, education, and awareness of its employees, business associates, and contractors, as appropriate.

Policy 800: Personnel Account Management

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN will ensure its personnel requiring access to Electronic Protected Health Information ("ePHI") have appropriate access rights.

Authorization and/or Suspension

1. WISHIN will identify all workforce members who require access to ePHI.
2. WISHIN will grant authorization to access ePHI as necessary based on job functions, based upon the roles performed.
3. WISHIN's Security Officer will supervise workforce members' ePHI access.

Workforce Clearance

1. All workforce members having access to ePHI will undergo an appropriate background investigation prior to employment, and be subject to ongoing, periodic background checks.
2. WISHIN shall maintain documentation regarding background checks, personnel actions, and the levels of access granted to each workforce member should be maintained for at least six years.
3. WISHIN will review access levels periodically as determined by the Security Officer, and when the status of a workforce member changes.
4. WISHIN will implement appropriate clearance procedures for temporary personnel and contractors.

Termination

Upon termination, WISHIN will complete the following tasks:

1. Give the former workforce member a copy of his or her signed confidentiality statement and notify the former member of his or her ongoing confidentiality duties.
2. Recover from the former workforce member all keys and access tokens for facilities, buildings, offices, desks, and file cabinets.
3. Disable the former workforce member's network access, e-mail accounts, and access to all other systems.
4. If the former workforce member had system level or administrative access to systems, change system passwords for all systems containing or allowing access to sensitive information.
5. If the former workforce member had remote system access, retrieve all hardware, software, and electronic information.
6. Change the former workforce member's voice mail message with information about whom to contact for assistance.
7. Review computer files and forward or destroy, as appropriate.

8. As appropriate, notify customers and vendors with ongoing issues or projects involving the former member that such member is no longer employed.
9. Determine appropriate dissemination of email communications, files, and other documentation retained by the former workforce member, regardless of the medium.

Policy 900: Information Access Management

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor.

Policy

WISHIN will grant participants access to the HIE as set forth in the Participant Agreements between the participants and WISHIN, and these Policies.

Access Authorization and Establishment

1. WISHIN will require the assistance of technical specialists from time to time to develop and maintain WISHIN's system. These individuals should have limited ongoing access monitored by the WISHIN Security Officer.
2. WISHIN Applications will incorporate controls for managing access to selected information and functions, including auditing capabilities.
3. Each user of the system will have a unique identification and be required to set up a complex password. The system should provide a method to accurately identify the user through a two-factor authentication process.[1] All systems should include identity authentication functions consistent with this policy and with the level of confidentiality of the information they contain or process.
4. The WISHIN Security Officer will establish the authority and ability to read, write, modify, update and/or delete information from automated files or databases. The Security Officer may grant a specific combination of authorities and abilities to specific users. The Security Officer should not give any authority or ability to users beyond their needs. The Security Officer should establish access rules or profiles in a manner that restricts users from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.
5. Computer operations which support sensitive information will operate in accordance with procedures approved by the Security Officer and assure that (i) information cannot be modified or destroyed except in accordance with procedures; (ii) operating programs prohibit unauthorized inquiry, changes to, or destruction of records; and (iii) operating programs are used to detect and store all unauthorized attempts to penetrate the system.
6. WISHIN will develop and approve procedures for temporary and emergency access.

Access Management

1. WISHIN may revoke access to the network to ensure the security, integrity, and availability of the network to other users.

[1] Two-factor authentication requires factors beyond general usernames and passwords to gain access (e.g., requiring users to answer a security question such as "Favorite Pet's Name") as defined in the HIPAA Security Guidance bulletin from the Centers for Medicare & Medicaid Services (CMS) on December 28, 2006.

2. Pursuant to any policies and procedures, participants must notify WISHIN when there is a significant change in duties that may require changes in access to information resources, including termination of relationships with WISHIN.
3. WISHIN will review access to ePHI and confidential information:
    - Periodically and no less than every year
    - When the status of a user changes
    - After six months of account inactivity
    - Access authorization is modified or terminated as necessary based on changes in job duties and changes in personnel
4. Where appropriate, WISHIN interface servers will log off users after a specified period of inactivity as established by WISHIN.

Policy 1000: Education, Training, and Awareness

Scope and Applicability: This policy applies to WISHIN.

Policy

WISHIN will communicate the information security and privacy policies and procedures of WISHIN to all workforce members and maintain a program to maintain effective awareness of information security policies and procedures.

Training/Notification of Policies

WISHIN will inform all workforce members of security and privacy policies and procedures and their responsibilities in writing. All new workforce members of WISHIN will sign a statement acknowledging they have received and read the security and privacy policies, understand their responsibilities, and have knowledge of the consequences of violations of security procedures.

Each WISHIN workforce member with access to critical systems and sensitive information will sign a signed statement of compliance on a periodic basis. The statement will indicate awareness, compliance, and intent of continued compliance with any information security and privacy policies.

WISHIN will train its workforce members on privacy policies upon their hire, and conduct subsequent training as necessary.

All users must be informed that any actions taken under their assigned identification, such as a user "ID," are their personal responsibility.

Communications of Policies

WISHIN will communicate important aspects of any information security and privacy policies and procedures on a regular basis through postings, distributions, logon screens, meetings, or other means that provide regular and useful reminders concerning information security and privacy policies and standards.

Persons responsible for information technology resources must be aware of the information security and privacy policies and procedures and must be knowledgeable about effective security practices for the technical environment under their control. In particular, WISHIN will train such individuals regarding password maintenance, incident reporting, viruses, and other forms of malicious software.

WISHIN will develop and disseminate guidelines and examples for users to assist in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, and should include but not be limited to information on passwords and password protection, logon IDs, and virus protection strategies.

Policy 1100: Access and Acceptable Use

Scope and Applicability: This policy applies to WISHIN.

Policy

All use of WISHIN's information technology is to be in compliance with this Plan, policies and procedures, and sound business judgment. WISHIN will monitor e-mail, Internet use, access to systems via mobile devices, and other computer resources.

Restriction of Access

WISHIN will develop, implement, and administer a procedure for restricting log-on access to individual terminals, workstations, and/or mobile devices to only those workforce members and authorized users that (i) follow the applicable log-on authorization procedures, and (ii) are actually authenticated as authorized users.

Use of the Internet, e-mail and other uses of computer resources must always be able to withstand public scrutiny and not cause legal liability or embarrassment to WISHIN and/or participants.

No Expectations of Privacy

WISHIN will make workforce members aware that they should have no expectation of privacy when using WISHIN resources or networks to access the Internet, e-mail, or otherwise using WISHIN computer and information resources.

E-mail

WISHIN will employ virus protection software on workstations to prevent transmission of viruses in e-mail attachments and media devices.

Workforce members should not use e-mail that is not secure or encrypted to send electronic protected health information or confidential information.

Unacceptable Use

Unacceptable uses of WISHIN's information technology include, but are not limited to:

- Violation of the privacy of other users and their data.
- Violation of the legal protection provided by copyright and licensing laws applied to programs and data.
- Attempts by members to monitor or intercept the files or electronic communications of other members or third parties.
- Attempts by members to hack or obtain access to systems or accounts they are not authorized to use.
- Use of other members' log-ins or passwords.
- Use of electronic media in a manner likely to cause network congestion or significantly hamper the ability of other members to access and use WISHIN's system.

- Use inconsistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state, or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene, or harassing material.
- Intentionally or knowingly releasing a virus or other program that damages, harms, or disrupts a system or network.
- Violation of the integrity of computing systems. For example, users will not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
- Use of the WISHIN computing facilities for fund-raising or public relations activities unrelated to an individual's employment by WISHIN.
- Malicious or disruptive use, including use of the WISHIN facilities or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use to make unauthorized entry to any other machine accessible via the network.
- Using WISHIN resources for unauthorized or illegal purposes or knowingly accepting or using information which has been obtained by illegal means.
- Use in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use.
- Misrepresentation of one's self or WISHIN.
- Accessing or attempting to access other data or information without proper authorization even if it is not securely protected.
- Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained.
- Sending an overwhelming number of files across the network (e.g., spamming or e-mail bombing).
- Preventing others from accessing services.
- Sending forged messages under someone else's user ID.

Workstation Security

1. Users are not permitted to install any unapproved software on, or transfer data to or from, any portable device or other storage media to their computer or workstation without specific approval.
2. WISHIN IT staff is responsible for conducting routine backups, installing and using virus protection routines, and installing patches and updates in accordance with WISHIN procedures.
3. WISHIN must ensure computer repairs are undertaken in a manner that protects the confidentiality of data stored in the system.

4. Workstations and drives or media devices, with critical and sensitive data stored on them or accessible through them, should be further secured (using software) against unauthorized use even by someone who has legitimate access to the physical space.
5. Equipment and/or confidential information may not be removed from the office area without WISHIN's prior approval.

Virus Protection

1. WISHIN users will employ virus protection on all workstations connected to WISHIN's networks, including those remotely accessing the network. Users will not attempt to turn off the virus protection nor alter the antivirus settings on WISHIN-managed workstations.
2. Workstations using antivirus software not centrally managed must have the antivirus software set to scan all files before allowing them to be accessed or changed. Such antivirus software must be configured to update its virus definitions at least weekly.
3. Because computer viruses have become so complex, users must not try to eradicate viruses without expert assistance. If a user suspects infection by a virus, they must immediately disconnect from the network or shut down their machine and then call the Help Desk.
4. Users should not open e-mail from an unknown, suspicious, or untrustworthy source, nor download any attachments from such e-mail.
5. Users should delete spam, chain, and other junk e-mail without opening or forwarding such e-mail.
6. Users should not forward virus warnings which they may receive via e-mail to friends or coworkers. Instead, users should forward such e-mail warnings to the Security Officer. Most of these warnings are hoaxes that accomplish the same results as actual viruses; they cause mass e-mailings.

Personal Use of WISHIN's Information Resources

WISHIN's information resources are to be used primarily for business purposes, only for the performance of one's job responsibilities.

Occasional and reasonable non-business usage of systems may be allowed at the discretion of management, provided such usage:

1. Does not interfere with work performance or productivity of oneself or others.
2. Does not consume more than a trivial amount of resources that could otherwise be used for business purposes.
3. Does not endanger the privacy or security of protected health information or confidential information.
4. Is not contrary to WISHIN's policies, standards or procedures.

Users are responsible for exercising good judgment regarding the reasonableness of personal use.

If there is any uncertainty about whether a use is appropriate or allowed, users should consult their supervisor or manager. The supervisor or manager may consult the Security Officer for further guidance.

WISHIN Implementation of the Health Information Exchange ("HIE").

Each user of the HIE will have a unique identification. The system will provide a method to accurately identify the user through a two-factor authentication process[2].

A self-service password recovery process may be used.

At the recommendation of the Security Officer, with the approval of the designated committee(s) of the Board, WISHIN may permit the following actions:

1. A participant to perform password management for its users
2. A participant to employ a single sign-on process for its users.

[2] Two-factor authentication requires factors beyond general usernames and passwords to gain access (e.g., requiring users to answer a security question such as "Favorite Pet's Name") as defined in the HIPAA Security Guidance bulletin from the Centers for Medicare & Medicaid Services (CMS) on December 28, 2006.

Policy 1200: Security Incidents

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor.

Policy

All security incidents will be reported to WISHIN's Security Officer, who will direct WISHIN and the contracted HIE vendor to take appropriate steps to block further incidents, repair and restore service, and preserve evidence.

Example Incidents

The following are examples of security breaches that apply to this policy. The list is not meant to be inclusive, but only a set of examples of what may constitute a security breach:

- Denial of service
- Virus attacks/malicious code
- Unauthorized access/activity
- Inappropriate usage
- Identity theft
- Equipment theft
- Violation of policy
- Unplanned downtime, depending on level of severity
- Data Integrity compromise/loss
- Failure of security
- Intrusion/attempted breach
- Interruption of operations
- Data compromise
- Adverse event
- Environmental event
- Disaster event with IT impact

Incident reporting

Any information concerning a known or suspected security breach (an "Incident") must be reported without delay and in writing. WISHIN will inform the appropriate participant's privacy and security contacts. In addition, WISHIN may, after consultation with legal counsel, report the incident to outside law enforcement authorities whenever this is required to comply with legal requirements, rules, or regulations.

WISHIN, in coordination with its contracted HIE vendor, will manage mitigation efforts, specifically, to:

1. Block or prevent continuation of the Incident, if possible
2. Repair the resulting damage and fix the root cause
3. Restore service to its former level, if possible
4. Preserve evidence, where appropriate

Investigation, Remedy, and Response

Upon receipt of written notice, WISHIN and its contracted HIE vendor will, without delay, identify and record any damage caused, restoration or repair required, and gather all of the necessary information required to prosecute the Incident, if applicable. WISHIN will develop a detailed plan to effectively remedy and respond to all reported Incidents pursuant to this policy. Additionally, WISHIN will develop, maintain, and update a database of reported Incidents with any effective remedies/responses in order to better protect WISHIN from similar or future information Incidents.

If a Participant's information, workforce member, or user was involved in an Incident, then the Security Officer will report such Incident to the privacy and security contacts designated by that participant:

1. WISHIN will coordinate with the participant's privacy and security contacts in responding to the Incident.
2. The appropriate response to an Incident will be determined by WISHIN and the participant's privacy and security contacts, and will based on the potential and/or actual impact of the incident.
3. Any harmful effects of the Incident will be mitigated to the extent practical.

Major Incidents will be immediately reported to the appropriate committee(s) designated by WISHIN.

Incident Response Plan

WISHIN will develop a detailed incident response plan. This plan will be reviewed by the appropriate committee(s) as designated by WISHIN.

Policy 1300: Physical Access and Security

Scope and Applicability: This policy applies to all facilities used by WISHIN and its contracted HIE vendor

Policy

WISHIN will implement physical safeguards to protect WISHIN personnel, information, data centers, equipment, and other assets.

Physical Access to Facilities and Controls

WISHIN will restrict physical access to areas within WISHIN facilities which contain servers or other storage devices containing protected health information or confidential information to those who have a need to have such access.

WISHIN will install reasonable and appropriate controls to control and validate each individual's access to facilities based upon the individual's role or function. Individuals may not enter areas where protected health information or confidential information is stored unless authorized.

Location of Terminals and Workstations

Terminals, workstations, printers, fax machines, and other peripheral equipment will be located in a secure area and be positioned in such a way as to minimize unauthorized overview.

Logs and Records of Access

WISHIN and its contractors will maintain appropriate logs and records of access.

Policy 1400: System Availability

Scope and Applicability: This policy applies to WISHIN and its contracted HIE vendor

Policy

WISHIN will develop, implement, and maintain appropriate procedures to respond to system emergencies or other occurrences (i.e., fire, vandalism, system failure, natural disaster, etc.), and to notify Participants of any system failure.

Data Backup

1. Back-ups of critical information and/or Electronic Protected Health Information ("ePHI") will be conducted in a manner to allow timely recovery of information.
2. Administrators are responsible for backing up each system and required to implement a tested and auditable process.
3. WISHIN or its contracted HIE vendor will store centralized services back-ups will on-site for quick recovery.
4. Critical business functions will also have back-ups stored in an off-site, secured commercial facility.
5. Application software will be copied to a separate back-up medium as new applications are added.
6. System software should be copied periodically and as major changes are made.

Disaster Recovery Plan

In the event of an emergency reaching the level of a "disaster," WISHIN will:

1. Activate its disaster recovery plan
2. Assess the impact to ePHI and operations
3. If necessary:
    a. Establish an alternate location for operations
    b. Secure replacement equipment
    c. Retrieve and restore back-ups from storage

Emergency Mode Operation

WISHIN will ensure the physical security of ePHI during emergency mode operations, limiting physical access to the extent practicable. WISHIN will ensure the technical security of ePHI via user identification codes and passwords to the extent practicable.

Testing and Revision

WISHIN's will test its disaster recovery plan (and revise as appropriate) periodically and whenever significant changes occur in the WISHIN information technology environment. WISHIN will maintain copies of the disaster recovery plan in multiple off-site locations. WISHIN will train workforce members in disaster recovery plan procedures.

Applications and Data Criticality Analysis

WISHIN will determine the ePHI most critical in the event of an emergency, and WISHIN will prioritize the systems and software used to access ePHI for restoration.