Iowa Health Information Network (IHIN)

SECURITY POLICIES
April 2017

IHIN Security Policies
Change History and Policy Approvals

Change History

Date:	Changes:
07/10/2013	1. Amendment 1- limiting the use of the query/look-up function for treatment purposes only and not payment and operations. Amendment 1 has an expiration date and other caveats for termination and is attached within this document. 2. Amendment 2 – makes confidential the results of the security risk assessment and the disaster recovery plan. This has been incorporated in Security Policies 10 and 11.
01/14/2015	1. Revised and updated the definition of HIPAA to include reference to the Omnibus Rule. 2. Throughout the document made edits to allow the Participant to apply equivalent standards of these policies to their BAA's and contractors. 3. Policy 5E – Changed this section to Authentication and identified additional NIST standards beyond that of passwords that may be used for user authentication.
06/30/2015	Amendment 1 – The Treatment Only period has been terminated with the passage of HF 381 which expands the allowable uses of the record locator service from just Treatment to Treatment, Payment and Health Care Operations as defined by HIPAA. This amendment and a link to HF 381 have been moved to the back of the document for historical reference.
4/1/17	Transition to private entity changes (replacement of references to IHIN and IDPH with IHIN)

Policy Approvals

Description:	Approved By:	Date:
Original Approval	State Board of Health	11/14/12
Amendments 1 & 2	State Board of Health	7/10/13
Full Review	State Board of Health	01/14/2015
Replacement of references to IHIN and IDPH with IHIN	IHIN	4/13/17

Table of Contents

Iowa Health Information Network (IHIN) Security Policies

INTRODUCTION

The purpose of these Security Policies is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the Iowa Health Information Network (IHIN). These Security Policies follow the principles of the core domains of the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.[1] To ensure continued compliance with applicable laws and regulations, these Policies will be periodically modified. Each Participant will have access to revisions and updates consistent with the requirements of the Participation Agreement. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies.

Compliance with all IHIN policies is a requirement for participation in IHIN. Each Participant must have established internal privacy and security policies and procedures that effectively manage access to, and the appropriate use of, Protected Health Information (PHI) and confidential data. Each Participant must ensure that its internal policies comply with all IHIN Security Policies. Participants may enact procedures that are more stringent than these policies, but must not allow those procedures to conflict with, or be less restrictive than these policies as they apply to IHIN.

The guiding security principles for IHIN are as follows:

Safeguards: PHI should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use or disclosure.

Accountability: Appropriate auditing mechanisms should be in place to report and mitigate non-adherence to policies and breaches.

Understanding Uses and Risks: Ongoing assessment of potential vulnerabilities and threats to security, advance planning, education and training, and other reasonable controls and risk minimization should be exercised to limit privacy and security threats.

Availability: Continuity of IHIN operations and contingency planning to limit exposure to security risks which could compromise system availability.

Minimization of Provider Burden: Reasonable ability for providers with a treatment, payment or health care operations reason to access patient records in a timely and efficient fashion without undue burden on provider workflow.

The primary objectives of these Policies are as follows:

[1] healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy_ security_ framework//1173

- To establish a secure and stable network environment.
- To effectively manage the risk of security exposure or compromise within IHIN.
- To communicate the responsibilities for the protection of information.
- To promote understanding and compliance with all applicable laws and regulations.

EFFECT OF LEGISLATION AND RULE CHANGES. The IHIN and Participants need to remain flexible in approach in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the HITECH Act.[2] These Security Policies will be reviewed, at minimum, every two years by IHIN.

[2] The Participants acknowledge the need to revise their policies and certain other technical and administrative features to conform to HITECH and regulations to be promulgated hereunder. Participants will make the required changes promptly as required by law.

DEFINITIONS

As used in these Policies and Standards, the terms set forth in this section shall have the meanings assigned to them below.

"Audit Trail" means a record that shows who or what system has accessed a computer system, when it was accessed and what operations were performed.

"Authorized Users" means those members of Participant's workforce (including employees, agents, contractors and any other persons having access to the IHIN by virtue of their relationship with Participant) who are individually authorized by Participant to have access to the IHIN to assist Participant in providing treatment, payment or healthcare operations and to whom Participant has assigned a unique identifier for access to the IHIN.

"Breach" means breach as such term is defined in the HIPAA Privacy Rule.

"Business Associate" or "BA" means a business associate as such term is defined in the HIPAA Privacy Rule.

"Business Associate Agreement" means the agreement posted on the IHIN's website, which may be amended from time to time by the IHIN and the Participant.

"Encryption" means the process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific need to know.

"Firewall" means a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

"HIPAA" means the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act, and the regulations promulgated thereunder, including, without limitation, the Privacy Rule, the Security Rule, the Breach Notification Rule, the Enforcement Rule, and the Final Omnibus Rule Modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, as any or all may be amended from time to time.

"HITECH Act" means Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), and the regulations promulgated thereunder.

"IHIN" means the Iowa Health Information Network, including all hardware provided, all software used or provided, all written specifications and user and technical manuals provided regarding the functionality and operation of the IHIN, and all data exchange and other services provided through the IHIN.

"IHIN's Authorized Personnel" means the IHIN's employees, agents and independent contractors under confidentiality obligations on terms substantially similar with the confidentiality provisions contained in this Agreement who are authorized by the IHIN to have access to the IHIN.

"Other Participants" means other entities that have access to the IHIN and have signed a Participation Agreement containing an obligation to comply with the Policies and Standards and to be responsible for any business associate, contractor or workforce member who accesses and uses the IHIN as Authorized Users on its behalf.

"Participant" means an authorized organization that has voluntarily agreed to enter into a Participation Agreement to access or use the IHIN.

"Participation Agreement" means the agreement entered into between the IHIN and a participant that prescribes the terms and conditions for access and use of the IHIN.

"Payer" or "Health Plan" means, but is not limited to, an insurance company, self-insured employer, government program, individual or other purchaser that makes payments for health services.

"Privacy Policies" and "Security Policies" means the IHIN's rules, regulations, policies and procedures for access to and use of the IHIN, which shall be posted electronically on the IHIN or otherwise furnished to Participant.

"Privacy and Security Workgroup" means the volunteer workgroup serving as a resource to the IHIN for the purpose of providing subject matter expertise for policies and procedures for the IHIN that will provide protections to consumers and providers.

"Privacy Rule" means the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

"Protected Health Information" or "PHI" means protected health information as defined in 45 C.F.R. § 160.103 that is created or received by an authorized Participant.

"Provider" means a person or organization that is a health care provider under HIPAA and is licensed or otherwise permitted to provide health care items and services under applicable state law.

"Public health activities" means actions undertaken by the IHIN in its capacity as a public health authority under HIPAA and/or as required or permitted by other federal or state law.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information available through the IHIN or interference with IHIN operations. As used in these policies, "Security Incident" includes attempted and successful privacy Breaches.

"Security Rule" means the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 CFR part 160 and subparts A and C of part 164.

"Subcontractor" means any third party engaged by the IHIN to assist in the design or operation of the IHIN or in the performance of the IHIN's obligations under this Agreement.

"TPO" means treatment, payment, or healthcare operations, as such terms are defined in the HIPAA Privacy Rule.

"Virus" means a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks.

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the control of such entity, whether or not they are paid by the covered entity.

IHIN Security Policy 1: *Compliance with Law and Policy*

Scope and Applicability: This Policy applies to all Participants.

Policy: Participants shall comply with all applicable laws and these Security Policies in accessing and using the IHIN.

Standards:

1. **Laws.** Each Participant shall, at all times, comply with all applicable federal and state laws and regulations, including, but not limited to, those protecting the confidentiality and security of Protected Health Information (PHI) and establishing certain individual privacy rights. Each Participant must use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

2. **IHIN Policies.** Each Participant shall, at all times, comply with these Security Policies. These Security Policies may be changed and updated by the IHIN upon reasonable written notice to Participants. Amendment(s) shall be effective when approved by IHIN. The IHIN shall notify Participants of all policy changes. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Security Policies.

3. **Participant Policies.** Each Participant is responsible for establishing internal policies that are necessary to comply with applicable laws and these Security Policies.

4. **Conflicting Policies**. In the event of a conflict between the IHIN's policies and the Participant's policies related to the IHIN, the IHIN's policies related to the IHIN shall control over Participant's policies, unless a Participant policy is more restrictive than the IHIN's policy, in which case the Participant's more restrictive policy will apply to that Participant only.

5. **Participant Criteria.** Each Participant shall be a HIPAA "covered entity" (as that term is defined under HIPAA) or Business Associate and thus subject to both its individual legal duty as a regulated covered entity under HIPAA and its contractually assumed obligations under the Participation Agreement.

6. **User Criteria.** Each Authorized User derives his or her permission to access and use the IHIN from a Participant. Therefore each Authorized User must maintain a current relationship to a Participant in order to use the IHIN. Authorized Users must therefore be one of the following: (i) Participant (for example, an individual physician) or Workforce of a Participant, (ii) an individual Business Associate (BA) or Workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or Workforce of such contractor or subcontractor. A Participant that is a covered Health Plan may also be an Authorized

User in its role as a third party administrator and BA for self-funded group Health Plans that are covered entities under HIPAA but are not themselves Participants.

7. **Application to BAs and Contractors.** Participants agree to apply standards to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Security Policy 2: *Information Stewardship*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy:
The purpose of the Security Policies is to provide a framework for protecting information. The IHIN shall provide a secure environment for the exchange of information through the IHIN and the protection of information held by the IHIN. The IHIN's services and internal operating processes and procedures will be in compliance with all applicable laws and regulations, as well as established industry practices. These Security Policies specify the terms of the relationship and the roles, rights and responsibilities of each Participant. Participants are responsible for ensuring their Authorized Users meet all privacy and security obligations in the Participation Agreement, which includes the IHIN Privacy Policies and the IHIN Security Policies.

Standards:
The IHIN is responsible for the following:

1. Protecting the information in IHIN from unauthorized access, destruction, or usage.

2. Managing the uses and risks associated with information available through IHIN. Making decisions about the permissible uses of information.

3. Providing and administering general controls such as back-up and recovery systems.

4. Establishing, monitoring and operating information systems.

5. Designing the IHIN system architecture to be a secure and redundant environment.

6. Requiring IHIN Contractors' compliance with all applicable federal and state privacy and security laws and regulations and these Security Policies.

7. Developing and implementing contingency plans as needed to avert stoppage.

8. Enforcing consequences associated with improper disclosure and other security related control deficiencies.

9. Authorizing Participants and entering into Participation Agreements with them.

10. Providing training and support for Participants using the IHIN.

11. Authorizing IHIN's Authorized Personnel to access to the IHIN and limiting their use of information in the IHIN for the purposes of system administration and Public Health Activities.

12. Reviewing and updating these Policies as needed, but no less than every two (2) years.

13. Reporting periodically to the Privacy and Security Workgroup and to the IHIN Executive Committee and Advisory Council regarding potential risks and mitigation strategies – as well as potential updates to these Policies.

14. Reporting significant system-related vulnerabilities and urgent privacy and security issues to the IHIN Executive Committee and Advisory Council in a timely manner.

15. Communicating significant modifications to information security and privacy policies and procedures through IHIN website postings, distributions to Participants, meetings or other means that provide regular and useful reminders concerning information security and privacy policies and standards.

Participants are responsible for:

1. Complying with the terms of the Participation Agreement, including the IHIN Privacy Policies and Security Policies, and all IHIN Policies and Standards.

2. Using the IHIN solely for purposes of treatment, payment, or healthcare operations (TPO) as further described in the IHIN Privacy Policies.

3. Training their Workforce prior to allowing access to IHIN.

4. Refraining from unauthorized or unacceptable access, use or disclosure of PHI.

5. Reporting all situations where they believe it is reasonably likely that a privacy or information security incident may exist to the IHIN Privacy and Security Officer or the hotline.

6. Implementing disciplinary action against and/or termination of access to the IHIN to any member of the Participant's Workforce found to have violated these Security Policies.

7. Cooperating with IHIN in compliance monitoring, auditing, and Breach investigations as requested.

8. Making this policy or standards equivalent to those in this policy applicable to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their Business Associate Agreements (BAAs).

9. Providing copies of Participant's privacy and security policies and procedures to the IHIN upon request.

10. Providing a list of Authorized Users, and associated roles if applicable, to the IHIN within five business days of the IHIN's request.

IHIN Security Policy 3: *Privacy and Security Governance*

Scope and Applicability: This Policy applies to the IHIN, the IHIN Board Committee and any established workgroups.

Policy: The IHIN shall be responsible for managing the daily privacy and security activities and issues of the IHIN.

Standards:
Responsibilities: The Privacy and Security Workgroup shall be responsible for providing overall direction and guidance regarding IHIN privacy and security and these Security Policies. Members of the Privacy and Security Workgroup will:

1. Make recommendations to the IHIN Board with regard to privacy, confidentiality and security policies and practices.

2. Review and recommend modification of privacy, confidentiality, and security policies and practices in light of operating experience, changes in law, and changes in available compliance tools.

The IHIN shall:

1. Develop Security Policies, with input from the Privacy and Security Workgroup.

2. Direct and review the findings from risk assessments and audits of information systems and privacy and confidentiality practices.

3. Lead the IHIN Security Incident Response Team to contain, investigate, and prevent future privacy, confidentiality, or security breaches.

IHIN Security Policy 4: *IHIN Privacy and Security Officer and Participant Security Point of Contact*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: The IHIN shall designate an IHIN Privacy and Security Officer who will be responsible for the operational aspects of these Security Policies. The Privacy and Security Officer shall have authority commensurate with his or her responsibilities. Participants shall designate a Security Point of Contact (POC) who will be responsible for the operational aspects of these Security Policies and who will be the Participant's single point of contact for the IHIN regarding security issues. The Security POC shall have authority commensurate with his or her responsibilities.

Standards:

The IHIN Privacy and Security Officer is responsible for operational matters regarding security and the day-to-day execution of these Policies. Specifically, the IHIN Privacy and Security Officer shall be responsible for the following:

1. Reviewing and recommending modification of these Security Policies and all supporting policies and procedures in light of operating experience, changes in federal and state law, and changes in available technology and compliance tools.

2. Monitoring changes to HIPAA and other state and federal privacy laws and analyzing new privacy and security regulations, for impact on IHIN operations.

3. Implementing and maintaining these Security Policies and other information security directives and policies as recommended by the Privacy and Security Workgroup.

4. Overseeing access control, disaster recovery, business continuity, incident response, and risk management issues and requirements of the IHIN.

5. Performing or overseeing the performance of ongoing information risk assessments and audits of IHIN systems.

6. Working with vendors, outside consultants, and other third parties to improve privacy protections and information security within the IHIN.

7. Receiving privacy and security complaints and reports of actual or suspected Security Incidents or Breaches of the IHIN and responding to questions from Participants and third parties regarding the Privacy and Security Policies and practices.

8. Participating on the IHIN Security Incident Response Team.

9. Monitoring the effectiveness of these Security Policies and incorporating the results of monitoring into recommendations for amendment or other action.

Participants are responsible for:

1. Designating a Security POC who shall be responsible for operational matters regarding security and the day-to-day implementation of these Security Policies.

IHIN Security Policy 5: *System and Technical Security Requirements*

5A: *Physical Access and Security*

Scope and Applicability: This Policy applies to the IHIN.

Policy: The IHIN will implement physical safeguards to protect information in the IHIN equipment, information and other assets.

Standards:
IHIN is responsible for the following:

1. Restricting physical access to all areas where IHIN infrastructure is located, including facilities which contain servers or other storage devices containing PHI or confidential information. Only IHIN's Authorized Personnel who have a need will have such access.

2. Installing reasonable and appropriate controls to validate each individual's access to facilities based upon their role or function. Individuals may not enter areas where PHI or confidential information is stored unless authorized.

3. Inventorying and tracking of all IHIN hardware and other assets utilized to support the IHIN.

5B: *Workstations and Other Devices*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: The IHIN and Participants shall use workstations in a manner to safeguard the confidentiality and integrity of PHI and confidential information.

Standards:
All workstations and other devices (including those accessed via secure, remote access) from or through which an Authorized User or IHIN's Authorized Personnel may access the IHIN must, at minimum, meet HIPAA standards for workstation security, including the following requirements:

1. Activity log. Participant shall maintain a log of all IHIN system access, including attempted log-ins, in such a way as to be able to identify both the user and the workstation used for this activity.

2. Network security. Internet connectivity and remote access of the IHIN must be secure.

3. Virus Protection. All workstations and other devices connected to the IHIN, including those remotely accessing IHIN, must provide up-to-date Virus protection. The IHIN and Participants shall employ Virus protection on all servers connected to the IHIN.

4. Viewing PHI. Users shall not leave workstations or devices logged into IHIN if they are unattended, and should not allow others to view PHI or confidential information on workstations or other devices unless the user knows they have a TPO reason to view such information. An automatic logoff after a pre-determined period of inactivity will be enforced on all confidential systems, where possible. The pre-defined period of inactivity will be determined for each individual application based on business needs, application parameters, and security risk assessments.

5C. *Encryption*

Scope and Applicability: This Policy applies to the IHIN.

Policy: All transactions through the IHIN, including all queries and responses, must be encrypted. The encryption technology must be configured in accordance with industry best practice to be secure against attacks.

Standards:
The IHIN shall:

1. Construct and maintain the IHIN technology platform to be compliant with data integrity requirements detailed in the Integrating the Healthcare Enterprise's[3] (IHE) document registration and audit trail specifications.

2. Ensure transactions through the IHIN are encrypted using transport layer security (TLS) protocol around IHE transactions.

5D: *User Logon IDs*

Scope and Applicability: This Policy applies to all Participants.

Policy: Each individual Authorized User shall have a unique logon ID and password for accessing the IHIN. An access control system shall identify each Authorized User and prevent unauthorized users from entering or using IHIN information resources.

Standards:
Participants shall verify all users are part of their Workforce and have a TPO need to access PHI through the IHIN. Participant shall authorize use and assign a logon ID to each Authorized User.

1. Security requirements for logon IDs include:
    i. Each user shall be assigned a unique identifier.

[3] http://www.ihe.net/Technical_Framework/index.cfm#IT

ii. Users shall be responsible for the use and misuse of their individual logon ID.

2. Participants will use or enhance existing role-based access privacy and security controls to restrict an Authorized User's access to information available through the IHIN based on the Authorized User's role and job function.

3. The logon ID for Providers accessing the IHIN through the Provider Portal will be locked or revoked after a maximum of three consecutive unsuccessful logon attempts. Passwords must then be reset by a self-service password recovery process using challenge questions or by the IHIN. This provision is not applicable to Authorized Users accessing the IHIN through the Participant's EHR system.

4. Workforce who desire to become Authorized Users of the IHIN must have a completed Participant's security training and signed an Authorized User agreement. Such agreement must be countersigned by the Participant.

5. Participant shall audit all user login IDs at least twice yearly and shall revoke all inactive logon IDs.

5E: *Authentication*

Scope and Applicability: This Policy applies to all Participants.

Policy: Participants shall require passwords or an equivalently strong and effective network authentication method for each and every Authorized User.

Standards:
Participant shall comply with the following when passwords are used for an authentication method:

1. Passwords shall conform to strong password guidelines as outlined by the National Institute of Standards and Technology[4]. An example of password criteria and requirements would be:
   i. The password must be a minimum of eight characters and contain a combination of upper case letters, lower case letters, numbers, and special characters.
   ii. The password should not be a word found in a dictionary (English or foreign)
   iii. The Password should not be a name, initials, birthdays, or phone numbers associated with the Authorized User.
   iv. Authorized Users shall not reuse their previous five passwords.
   v. Authorized Users should be required to change passwords at least every six months.

2. Participant may employ a single sign-on process for its Authorized Users.

[4] http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

3. Participant may use a self-service password recovery process.

4. Authorized Users shall safeguard their passwords to prevent unauthorized use and access to the IHIN.

4. If an account or password is suspected to have been compromised, Participant shall require an Authorized User to report the incident to Participant's Security POC and to change the password promptly.

When authentication methods other than passwords are used, Participants shall follow and comply with the guidance within NIST Special Publication 800-63-2: Electronic Authentication Guideline to implement a strong and effective authentication control.[5]

[5] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

IHIN Security Policy 6: *Information Access Management*

Scope and Applicability: This Policy applies to all Participants.

Policy: The IHIN shall grant Participants access to the IHIN as set forth in the Participant Agreement and the IHIN Privacy and Security Policies and Procedures. Participants shall grant only Workforce members with a TPO need will be granted access to IHIN, and shall have policies in place to prevent unauthorized persons from accessing the IHIN.

Standards:

Authorization to use IHIN. Participants shall:

1. Verify identity and authority of Workforce prior to granting access to IHIN.

2. Only grant access to the IHIN to Authorized Users who have a TPO need to access the IHIN.

3. Ensure that computer systems which access the IHIN operate under policies that:
    i. Prohibit unauthorized inquiry, changes or destruction of records; and
    ii. Meet HIPAA standards regarding the detection and recording of unauthorized attempts to penetrate the system.

Access Management.

The IHIN Privacy and Security Officer or the Security POC for any Participant may revoke access to the IHIN to protect the security, integrity, and availability of the IHIN to other users.

1. Participant shall review access to IHIN:
    i. No less than annually.
    ii. When the status of an Authorized User changes.
    iii. After six months of Authorized User account inactivity.

2. Participant shall modify or terminate access authorization as necessary and within a reasonable timeframe based on:
    i. Violations of law, the Participation Agreement, IHIN Privacy Policies, or IHIN Security Policies.
    ii. Changes in job duties and personnel.
    iii. Disciplinary actions.

IHIN Security Policy 7: *Security Awareness and Training*

Scope and Applicability: This Policy applies to all Participants.

Policy: All Authorized Users shall be required to complete security awareness training, which shall include the IHIN Privacy Policies and the IHIN Security Policies applicable to Authorized Users, and enter into an Authorized User agreement prior to being allowed to access the IHIN.

Standards:
Participant shall:

1. Provide a training program that includes, without limitation, acceptable and unacceptable uses of the IHIN (as further described below), password establishment and maintenance, software malfunction reporting, and the prevention, detection, containment, and eradication of Viruses and malicious software. Participant shall require Workforce who will have access to the IHIN to attend the training prior to providing them with a user ID and password for the IHIN.

2. Provide additional training to Authorized Users as needed in response to environmental and operational changes impacting the security of IHIN, e.g., addition of new hardware or software, increased threats.

3. Include an IHIN training component in Participant's regular security training program.

4. Require all Authorized Users to enter into an Authorized User agreement prior to being granting access to the IHIN. The Authorized User agreement shall include, without limitation, an acknowledgment that the Authorized User has received and read the IHIN Privacy Policies and IHIN Security Policies and understands their responsibilities under them and the consequences of violating them.

5. Include in Participant's privacy and security policies and Participant's Authorized User training programs information on the reporting of reasonably likely security incidents and to the Participant's Security POC and/or to the IHIN security hotline (800-774-0388) as quickly as possible.

6. Maintain appropriate documentation of all training activities and current and historical signed Authorized User agreements for at least seven years.

7. Distribute security reminders and special notices to Authorized Users regarding urgent issues which could affect the IHIN, such as new threats, hazards, vulnerabilities, and/or countermeasures.

Unacceptable Uses.
Unacceptable uses of the IHIN include, but are not limited to, the following:

1. Violation of the legal privacy protections of other Authorized Users, Other Participants, patients and/or their data.

2. Violation of the legal protection provided by copyright and licensing laws applied to software and data.

3. Unauthorized attempts to monitor or intercept the files or electronic communications of Other Authorized Users, Other Participants or third parties.

4. Attempts to hack or obtain access to systems or accounts the user is not authorized to use.

5. Obtaining or possessing (except for the Participant's creation and issuance of passwords to Authorized Users or password recovery), using or attempting to use someone else's password regardless of how the password was obtained.

6. Deliberately causing the IHIN to crash or taking other measure to compromise the confidentiality, integrity or availability of the IHIN.

7. Attempting to break into an information resource or to bypass a security feature of the IHIN. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.

8. Introducing, or attempting to introduce, computer Viruses, Trojan horses, peer-to-peer or other malicious code into the IHIN or into an information system connected to the IHIN.

9. The willful, unauthorized access, disclosure or inspection of confidential or sensitive information to which Workforce has not been approved.

10. Using of electronic media in a manner that is likely to cause network congestion or significantly hamper the ability of other members to access and use the IHIN.

11. Using the IHIN in a manner inconsistent with applicable laws and regulations and the express purposes of the IHIN.

12. Misrepresenting the user's identity on the IHIN.

IHIN Security Policy 8: *Information Systems Audit Controls*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Audit Controls are technical mechanisms that track and document computer activities. This Policy is designed to detect misuses of information and inappropriate or illegal access or disclosures of PHI. Having effective auditing and logging practices and preserving an Audit Trail can foster trust among patients and the general public in knowing that their data are being used only in appropriate ways.

The IHIN and all Participants shall review IHIN activity on a routine basis to monitor intentional or unintentional connections and disconnections to the IHIN, queries sent from Participants to the master patient index (MPI), and records retrieved by Participants through the record locator service (RLS). Hospitals, group practices, individual physicians, and other providers already maintain auditing requirements established through HIPAA and the HITECH Act. These laws require providers to log and maintain an Audit Trail of every access, use and change to a patient record. This policy extends these auditing requirements to users of the IHIN.

Because IHIN is primarily decentralized and is involved in the exchange of health information from one Participant to another through the IHIN, the IHIN Audit Trails will identify organization-level activity. Participants shall identify and report activity at the Authorized User level.

Standards:
IHIN shall:

1. Determine audit requirements for IHIN and Participants, including the data elements to be maintained for auditing purposes and the audit data and reports regarding IHIN activity that Participants are required to submit to the IHIN. Examples of information system activity data and documents may include, but are not limited to, Audit Trails, activity reports, and Successful Security Incident reports.

2. Establish a process for Participants to submit audit data and reports to the IHIN Privacy and Security Officer.

3. Secure all original Audit Trails from the IHIN and Participants in a secure location and in a tamper-proof format accessible only by the IHIN Privacy and Security Officer or his/her designee.

4. Maintain all original Audit Trails for at least seven years.

5. Review Participant use of IHIN, including Audit Trails, on a periodic basis for suspicious activity and possible violations.

6. Review Authorized User accounts for Participants using XUA. IHIN shall review the query requests (e.g., who was the Participating organization sending the information and which patient did the query involve?).
    i. If IHIN identifies suspicious activity it will provide Participant with information about the potentially inappropriate use, disclosure or access of PHI.
    ii. IHIN will coordinate any follow-up on the suspicious activity with the appropriate Participant.
    iii. IHIN will provide Participants assistance in the procurement of further detail not included in the standard Audit Trail information. Additional ad hoc reports can be requested from and defined by the IHIN as needed.

7. Request and review Participant Audit Trails and reports on a regular basis. Unusual activity and possible violations will be documented and appropriate mitigating action will be taken and documented, consistent with the provisions of the HIPAA Security Rule.

8. Breaches identified as a result of information systems activity review shall be investigated as outlined in the IHIN Security Incident Response Plan.

9. A summary of the findings from these review activities shall be reported to the IHIN Privacy and Security Workgroup on an annual basis.

Participant shall:

1. Routinely audit its Authorized Users' activities in order to assess potential risks and vulnerabilities with regard to PHI and the IHIN.

2. Have an audit/system activity review policy which defines the roles, responsibilities, and expectations regarding system logging, log retention, analysis, review, and reporting.

3. Log and review IHIN Authorized User accounts and traffic. At minimum, the following activities shall be examined:
    i. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    ii. File accesses – Scan successful and unsuccessful file or record access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file or record creation, modification, or deletion.
    iii. Security Incidents – Examine data from security devices or system Audit Trails for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., Viruses, worms), denial of service, or scanning/probing incidents.
    iv. User Accounts – Review Authorized User accounts within all systems to ensure users who no longer have a business need for access and use of the IHIN no longer have access to it.
4. Maintain Audit Trails to track individual Authorized User activity and activity for all workstations and other devices (including those accessed via secure, remote access) from or through which a connection to IHIN may be made.

i. The Audit Trails shall identify, at a minimum: 1) individual log-in identification (user ID); 2) position of the individual (if requested by the IHIN); 3) date and time; 4) patient account that was accessed; 5) all log-ins, successful and failed; and 6) the IP address of the connection, if available.
ii. Audit Trails shall be retained in a secure location for a minimum of seven years.

5. Analyze and review Audit Trails and activities by Authorized Users at a minimum quarterly to verify compliance with these Security Policies and terms of the Participation Agreement.

6. Create Audit Reports summarizing IHIN user activity. Reports shall use a standard data file format (e.g. txt, csv, xls, etc), and include the following data elements:
   i. Reviewer's name;
   ii. Date and time of performance;
   iii. Time frame, scope, data used for the report and other contextual information necessary to understand the findings of the report (i.e., to describe what information was analyzed and for what time frame);
   iv. Significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). Provide Audit Reports to IHIN within two business days of its request.

7. Participant shall cooperate with IHIN in any audit, including, but not limited to, providing IHIN with access to any data, documents or system reasonably necessary for IHIN to evaluate the Participant's compliance, making personnel available to discuss the Participant's processes and procedures, and making space available on-site for IHIN's Authorized Personnel to conduct the audit.

IHIN Security Policy 9: *Security Incidents, Notification, Investigation and Mitigation*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: The IHIN and all Participants shall investigate, respond to and report known or suspected Security Incidents related to the IHIN in compliance with applicable federal and state law and in accordance with the Participation Agreement the IHIN Privacy Policies and these Security Policies.

Standards: The Participant shall:

1. Instruct Workforce that any information concerning a known or suspected Security Incident must be reported to the Participant's Security POC without delay.

2. Notify the IHIN of any confirmed or reasonably likely security incidents or breaches as soon as practicable but no later than seven days after it is known to the Participant, with as much information as available and keep IHIN apprised of information gathered throughout Participant's investigation.

3. Submit a written report to the IHIN summarizing confirmed Breaches and confirmed Successful Security Incidents including response, remedies (completed or in process) and consequences for Participant's Workforce implicated in the incident within sixty days after a Breach notification to the IHIN. Maintain the reports for at least seven years.

4. Take immediate action to contain and prevent continuation of the Breach to the extent possible.

5. Address the root cause of the Breach and any discovered weaknesses in Participant's information systems and security policies or practices.

6. Develop, maintain and update a database of reported known or suspected security incidents with any effective remedies/responses and provide to the IHIN upon request.

The IHIN shall:

1. Develop the IHIN Security Incident Response Plan, with input from the Incident Response Team and the Privacy and Security Workgroup.

2. Provide a toll-free telephone hotline, available 24/7/365, for reporting known or suspected Security Incidents.

3. Activate the IHIN Security Incident Response Team, as needed to respond to known or reasonably likely Security Incidents.

4. Serve as a resource to Participants who have Breaches involving or impacting the IHIN.
    i. Facilitate information sharing between Participants to aid in fact-finding and investigating known or suspected Security Incidents.
    ii. Provide information regarding risk mitigation, containment, and ameliorative action.

5. Enforce the IHIN Participation Agreement (including suspension and termination of access).

6. Preserve and maintain Audit Trails and information regarding confirmed Breaches.

7. Require modifications to IHIN system architecture and applications when Breaches have exposed vulnerability.

8. Take remedial actions appropriate to the Breach for IHIN's Authorized Personnel implicated in a Breach.

IHIN Security Policy 10: *Risk Assessment and Management*

Scope and Applicability: This Policy applies to the IHIN and Participants.

Policy: The IHIN and Participants shall conduct an initial security risk assessment and subsequent risk assessment(s), as provided in this policy.

Standards:
The IHIN shall:

1. Develop a Security Risk Management Plan to identify potential risks/threats to and vulnerabilities of the security of the IHIN and the risk of disruption of IHIN services and to develop appropriate mitigation strategies and activities. The resulting Plan will also include audit recommendations, if appropriate. The Risk Assessment Plan shall:
    i. At minimum, address identification of threats, vulnerabilities, impact that may occur, and likelihood of harm.
    ii. Address natural (e.g., floods, storms), human (e.g., intentional or accidental), and environmental (e.g., power surges, hazmat contamination) threats.
    iii. Address risk monitoring and response.
    iv. Be approved by the Privacy and Security Workgroup and the IHIN Breach.

2. Conduct periodic risk assessments. The IHIN Privacy and Security Officer shall ensure that a risk assessment is conducted twice per year, at minimum, and a report is developed to document the issues and concerns discovered, as well as recommendations for addressing the concerns. The risk assessment shall:
    i. Comply with Risk Assessment guidelines set forth by NIST 800-30 (revision 1)[6] or similar protocols.
    ii. Define activities and processes which are to be included in the risk assessment, with input from the IHIN Infrastructure and Services Workgroup and, as appropriate, the IHIN Security Incident Response Team.
    iii. Identify the potential risks and vulnerabilities to the confidentiality, integrity and availability of critical data and information technology.
    iv. Identify potential means to mitigate such risks and vulnerabilities.
    v. Identify areas where these Security Policies may fail to satisfy the requirements of the Security Rule and other applicable information security laws, industry standards and regulations.
    vi. Document and maintain the methodology and results of Risk Assessments.
    vii. The periodic risk assessment reports of findings and concerns, recommendations, and mitigation strategies as described in this Standard 2 shall be confidential records pursuant to Iowa Code §22.7(50) (2013).

3. Re-assess risks, as needed, after Security Incidents and/or Breaches, and as vulnerabilities are identified by the IHIN Incident Response Team.

[6] http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

i. Once immediate steps are taken to mitigate the risks associated with the Security Incident or Breach, the IHIN Privacy and Security Officer will investigate the cause and evaluate the impact on the IHIN.
    a. If necessary, this will include a security audit of IHIN physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken by Participant(s) involved in the Security Incident or Breach.

ii. The IHIN Privacy and Security Officer will make recommendations to put into effect adequate safeguards against further Security Incidents or Breaches. These may include:
    a. Updating these Security Policies and/or the terms of the Privacy Policies or Participation Agreement.
    b. Enforcing and/or modifying the IHIN vendor contract to ensure desired safeguards are effectively implemented.

iii. Reviewing and updating procedures to reflect the lessons learned from the Incident Response investigation.

4. Re-assess risks whenever significant changes occur in the IHIN's information technology environment.

5. Re-assess risks as industry business practices, technology, and standards change and as vulnerabilities become apparent.

The Participant shall:

1. Prior to connecting to the IHIN, identify potential risks/threats relating to Participant's connection to the IHIN, including risks/threats that may affect PHI available through the IHIN, and develop appropriate mitigation strategies and activities to address identified risks/threats.

2. Risk assessments should include an evaluation of Participant's existing physical and technical security measures and an assessment of the adequacy of controls within the Participants' network, operating systems and applications related to Participant's connection to the IHIN.

3. Re-assess risks at least annually and: (a) as needed after Security Incidents and/or Breaches; (b) as material vulnerabilities are identified; (c) as industry business practices, technology and standards change in a manner that may affect Participant's security policies or procedures with respect to the IHIN; and (d) when applicable laws and regulations regarding information system security are enacted or changed.

4. Document the risks and vulnerabilities discovered during risk assessments, develop recommendations for addressing the concerns, and implement the changes reasonable and appropriate necessary to address the identified risks and vulnerabilities.

IHIN Security Policy 11: *Disaster Recovery Plan*

Scope and Applicability: This Policy applies to the IHIN.

Policy: The IHIN shall develop, implement and maintain appropriate procedures to respond to IHIN system emergencies or other occurrences (e.g., fire, vandalism, natural disaster, etc.). The IHIN shall periodically assess potential risks and vulnerabilities to the IHIN as described in Security Policy 10 and develop a Disaster Recovery Plan to maintain the essential functions of the IHIN during an emergency.

Standards:

The IHIN shall:

1. Develop a Disaster Recovery Plan which shall:
   i. Determine business processes and recovery criticality.
   ii. Be based on results of testing, experience and evolving technology.
   iii. Create contingency strategies.
   iv. Include Plan testing, training and exercises.
   v. Address natural (e.g., floods, storms), human (e.g., intentional or accidental), and environmental (e.g., power surges, hazmat contamination) threats.
   vi. Provide for Disaster Recovery Plan review and updates.
   vii. Be consistent with NIST sp 800-34 contingency planning guidelines.[7]

2. Create a redundant environment. IHIN is designed so that there is a redundant environment in a different geographic location from the IHIN where active virtual servers are established to distribute processing load and provide fail-over capabilities in case of a disruption.

3. Provide for IHIN applications and data back-up. Back-ups of critical information shall be conducted in a manner to allow timely recovery of information.

4. Test the Disaster Recovery Plan periodically and whenever significant changes occur in the IHIN information technology environment.
   i. The IHIN shall test backup procedures on an annual basis to ensure that exact copies of applications and data from the IHIN can be retrieved and made available.
   ii. To the extent such testing indicates need for improvement in back-up procedures, the IHIN shall identify, document, and implement such improvements in a timely manner.
5. Train its Authorized Personnel in Disaster Recovery Plan procedures.

6. Perform applications and data criticality analysis. The IHIN will establish priority for restoration for systems and applications used to access critical information.

---

[7] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf