



# Statewide Health Information Exchange Privacy and Security Framework Overview of HIE Policies

## Table of Contents

Background .....	2
Purpose .....	3
Scope .....	3
Definitions.....	3
Overarching Privacy and Security Assumptions .....	3
Iowa's Statewide Health Information Exchange (HIE) .....	4
Authorization .....	5
Authentication .....	5
Role-based Access .....	6
Audit .....	6
Participation agreements .....	8
Individual Choice to Participate in the Statewide HIE .....	9
Disclosure limitation .....	11
Compliance with Health Insurance Portability and Accountability Act of 1996 .....	12
Openness and transparency .....	12
Monitoring of usage and enforcement of HIE policies .....	13
Limitation of Liability/Immunity .....	13
Reconciliation with Other laws .....	13
Contact Information and Procedures .....	15
Frequently Asked Questions .....	15



## Background

The statewide health information exchange (statewide HIE) is a public and private collaboration created to facilitate the electronic exchange of health information between health care participants. The statewide HIE provides fast, secure and reliable exchange of health information among system participants (e.g., patients, providers, payers, public health) across the state. The statewide HIE is not a medical database or storage facility for medical records. It is a mechanism to facilitate the movement and delivery of health information among those with a need to know. The design and implementation of the statewide HIE includes strong security precautions to safeguard personal health information.

With the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in February 2009, as part of the American Recovery and Reinvestment Act (ARRA)<sup>1</sup>, the federal government has made health information technology (health IT) a national priority. Two significant components of health IT are electronic health records (EHR) and health information exchange (HIE). EHRs are used to collect and store health information and an HIE facilitates sharing of essential health information from EHRs across the boundaries of provider settings. Together, EHRs and a statewide HIE will allow health care providers access to real-time health information. Real-time health information helps *providers* make the best health care decisions and provides *patients* with continuity of care regardless of the provider they visit. A key premise, according to Dr. David Blumenthal, National Coordinator for Health Information Technology, is “information should follow the patient, and artificial obstacles – technical, business related, bureaucratic – should not get in the way.”<sup>2</sup>

*Importance of Policymaking:* For a statewide HIE to be successful, patients must trust their health information is kept confidential and secure, and providers must be able to access their patients’ information to make the best health care decisions. Privacy policies and HIE security controls provide assurances to patients; however it is important to find the right balance in policymaking to allow providers access to the information they need to help their patients. Strict privacy policies can slow the adoption of the statewide HIE and decrease the value of the exchange for providers. Policies that are too lenient can negatively impact the integrity of the statewide HIE and reduce trust and perceived value of the exchange of health information.

*Opportunity to be More Secure:* There are some potential risks associated with electronic health information (e.g., data entry errors, data and identity theft). However, there are similar risks with paper record processes. Current EHR and HIE technology has the opportunity to provide greater privacy and security protections than previously possible with traditional record systems. Unlike paper health records, certified EHRs are password protected and encoded to ensure only authorized personnel (or participants) have access to health information. An audit log automatically records when and by whom an EHR is viewed, modified, or shared. Data backups regularly archive health data, and in the event of a disaster (e.g., flood, fire, tornado), files can be easily restored to the original location, or an alternate setting.

The statewide HIE privacy and security policies were developed by the Iowa e-Health Executive Committee and Advisory Council with special assistance from Iowa e-Health’s multi-stakeholder Safeguard Privacy and Security Workgroup. This workgroup included attorneys and privacy and security experts that were involved in Health Information Security and Privacy Collaboration (HISPC). The workgroup reviewed privacy and security policies best practices from several other states (e.g., Minnesota, Delaware, Alaska, Nebraska) and reviewed recommendations and findings that were a result of HISPC.

---

<sup>1</sup> American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, (February 17, 2009). Division A Title XIII: Health Information Technology for Economic and Clinical Health Act (HITECH).

<sup>2</sup> Dr. David Blumenthal, email to Health IT News e-mail list, November 12, 2009, [http://healthit.hhs.gov/portal/server.pt?open=512&objID=1406&parentname=CommunityPage&parentid=23&mode=2&in\\_hi\\_userid=11113&cached=true](http://healthit.hhs.gov/portal/server.pt?open=512&objID=1406&parentname=CommunityPage&parentid=23&mode=2&in_hi_userid=11113&cached=true).



## Purpose

Personal privacy is of critical importance. The statewide HIE complies with state and federal laws, including HIPAA, as applicable. With the assistance of Iowa's legal counsel, the Iowa e-Health Safeguard Privacy and Security Workgroup, previous work by the Health Information Security and Privacy Collaboration (HISPC) project, the Office of the National Coordinator for Health IT (ONC), the Iowa e-Health Executive Committee and Advisory Council, and the Iowa e-Health Consumer Interest Group, Iowa e-Health has established policies that balance the participants' rights and expectations with the need for relevant information to support informed decisions and better quality health care.

The intent of these policies is to:

- 1) Provide information about participants' rights regarding the use and disclosure of their personal health information
- 2) Establish an appropriate level of security to protect participants' data from unauthorized access and disclosure. These policies define the access controls and parameters necessary to achieve this protection and to provide for the secure and reliable operation of the statewide HIE.
- 3) Align with the Nationwide Privacy and Security Framework released by ONC in December 2008. The principles outlined in the Nationwide Privacy and Security Framework have served as a guide for Iowa and other public and private-sector entities establishing statewide HIEs. More information about ONC's Privacy and Security resources is available at <http://healthit.hhs.gov/>.

## Scope

These policies are applicable to all participants of the statewide HIE. Organizational 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.

## Definitions

*To be developed.*

## Overarching Privacy and Security Assumptions

- Iowa e-Health will require all participants to sign a standard participation agreement, either individually or through their authorized organization. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each participant. The signing of the agreement means that each participant will adhere to the policies and procedures of the statewide HIE.
- Iowa e-Health will define the type of health information to be exchanged, and services to be accessed, by participants.
- Iowa e-Health will exchange health information using national standards for data content and data definitions.
- All participants will have adopted and implemented privacy and security programs, policies, and procedures as required by law to ensure the confidentiality, integrity, and availability of health information.
- A participant may be asked at any time to validate that they have appropriate policies and procedures in place and to provide evidence of compliance with these policies and procedures.



## Iowa's Statewide Health Information Exchange (HIE)

An HIE allows providers to access vital patient information where and when it is needed. An HIE is a hub that connects different EHR or other clinical information systems. The statewide HIE is not a central data repository where all patient records are stored. The statewide HIE facilitates the transfer of health information between care providers, unless a patient requests to opt-out of the exchange.

Iowa's statewide HIE enables structured EHR data to be securely shared among a patient's health care providers (e.g., clinics, hospitals, pharmacies, etc). The information can be shared without relying on fax machines and without burdening patients by asking them to carry paper files or electronic files stored on a CD to give to another provider.

### *What information will be available through the statewide HIE?*

Once the statewide HIE is established, Iowa must determine the HIE services (data transactions) to facilitate through the exchange. The multi-stakeholder, public-private Iowa e-Health Executive Committee, Advisory Council, and workgroups have been discussing and prioritizing potential HIE services. The following list represents the type of information providers will be able to view and access through the statewide HIE:

- Clinical care summaries (e.g., the ability for providers to view a continuity of care document, discharge summary, and/or referral summary in real time)
- Medication history (e.g., the ability to view medications previously dispensed to a patient, including prescriptions from other providers)
- Electronic reporting of immunizations administered (e.g., the ability to submit immunization data directly from a provider's EHR to the public health department) and immunization history (e.g., the ability for providers to electronically receive an immunization history from the public health department)
- Laboratory results (e.g., the ability to transfer of a lab result from the lab back to the ordering provider or perhaps another provider that wants to reference the lab result so they don't have to repeat the test)
- Electronic submission of quality metrics (e.g., the ability to submit measures required by Medicaid and/or Medicare for the meaningful use provider incentive program)

### *Who will have access to information available through the statewide HIE?*

Initially, the statewide HIE will facilitate exchange of treatment-related information between a patient's providers (e.g., physicians, hospitals, labs, pharmacies) and as required by the public health department (e.g., immunizations and reportable diseases). Over time, advanced HIE functionality may facilitate the exchange of health information for purposes other than treatment. Privacy and security policies and procedures will provide granularity to restrict access only to authorized participants with a legitimate need to view the information.

### *What is available for patients?*

As the statewide HIE matures, Iowa e-Health plans to implement a patient portal. Patients will be able to use the patient portal to access the same health information available to their providers. Until this functionality is available, patients may access their health information through their provider or health care organizations. As part of the meaningful use incentive program, providers must "provide patients with timely electronic access to their health information (including lab results, problem list, medication lists, and medication allergies) within four business days of the information being available to the provider." Some provider organizations are implementing patient portals through their EHR system to share this information with patients, while other provider organizations may make this information available through other means which will allow the patient to save or upload information into a personal health record. Similar to procedures today, if a patient notices inconsistent or incomplete information within their record, they will be directed to contact their provider directly to make the corrections.



## Authorization

All participants having access to the statewide HIE will have a unique ID. It is an organizational participant's responsibility to authorize, maintain, and terminate their employees' permission to use the statewide HIE. Iowa e-Health will be responsible for authorizing independent participants.

### *Proposed Policies:*

1. All participants having access to health information through the statewide HIE will have a unique participant ID for accessing health information.
2. Consistent with the authentication principles, each participant ID for accessing health information shall require at least two levels of authentication to access health information.
3. It is the organizational participant's responsibility to authorize and maintain access to health information. Iowa e-Health will authorize, maintain, and terminate an independent provider participants' access to patient health information.
4. The statewide HIE and all participants shall develop and accept security credentialing guidelines for their personnel that minimally include: 1) verifying the identity of individuals authorized to access/exchange health information; 2) assigning the appropriate role-based access for individuals authorized to access/exchange health information; and 3) providing individuals the mechanisms and training for access to the statewide HIE in compliance with statewide HIE principles and policies.
5. All organizational participants shall provide a list of all authorized users upon request by the statewide HIE within 24 hours
6. The statewide HIE and all organizational participants shall conduct a periodic review of authorized users to ensure user accounts are current and appropriate

## Authentication

A participant's identity will be verified at the time of log-in to the statewide HIE. The level of authentication required for all participants may vary depending on the participant's role-based access and the type of information being requested (i.e., participants with access to more information may be required to have more levels of authentication)

Participants with a direct connection to the statewide HIE (i.e., through an integrated EHR) and participants using the web-based portal through a secure organization connection (e.g., VPN), must be able to provide two levels of authentication. This includes at least one level of authentication for the organization, and at least one level of authentication for the individual user. Patients accessing their information through the patient portal will also be required to provide two levels of authentication, which will be similar to practices commonly used in the banking and credit card industry (e.g., a combination of username/password and personal security questions).

### *Proposed Policies:*

1. Organizational participants will have processes in place to authenticate the identity and role(s) of personnel before transmitting a participant's request for health information through the statewide HIE. For independent participants, the statewide HIE will have processes in place to authenticate the identity and role(s) of participants before transmitting a participant's request for information through the statewide HIE.
2. The statewide HIE shall require at least two levels of authentication to access health information.
3. The statewide HIE may provide single-sign-on capabilities for participants accessing the statewide HIE through an integrated EMR. Single-sign-on will not be available for participants accessing the statewide HIE through an HIE portal.
4. The statewide HIE and all participants must comply with National Institute of Standards and Technology standards for password usage.

*A workflow diagram is being developed to show how the recipients of confidential information will be authenticated.*



## Role-based Access

With role-based access controls, participants will be restricted to functionality and information available through the statewide HIE based on individual role and job function. Initially, the statewide HIE will facilitate exchange of treatment-related information between a patient's providers. As the statewide HIE matures, advanced HIE functionality may facilitate the exchange of health information for purposes other than treatment (e.g., quality reporting and population health). Privacy and security policies and procedures will provide granularity to restrict access only to authorized participants with a legitimate need to view the information.

### *Proposed Policies:*

1. Participants shall only access information for patients with whom they have a treatment relationship, and then only the health information relevant to the treatment being provided.
2. Organizational participants will administer role-based access for its authorized users. Iowa e-Health will administer role-based access for authorized administrators of the statewide HIE and independent participants.
3. Organizational participants will use or enhance existing role-based access privacy and security controls to restrict a participant's access to information available through the statewide HIE based on the participant's role and job function.
4. The statewide HIE will disable access to the statewide HIE for any participant inappropriately accessing health information.
5. The statewide HIE will conduct reasonability checks and terminate a participant's session due to inactivity and/or unusual use patterns.

## Audit

*Participants will comply with audit and compliance requirements that monitor what information was accessed through the statewide HIE, by whom, when and for what purposes.*

Monitoring system events [e.g., intentional or unintentional connections and disconnections to the statewide HIE, queries sent from participants to the master patient index (MPI), or records retrieved by participants through the record locator service (RLS)], is an essential safeguard for the statewide HIE infrastructure and important for building trust and confidence in health information exchange. Reports or alerts generated from audit records of the MPI and RLS can be used to provide transparency in how health information has been accessed or exchanged and can help monitor the appropriateness of activities.

The amount of information available in the statewide HIE audit logs is minimal compared to the audit logs maintained by providers' EHR systems. Hospitals, small group practices, individual physicians, and other providers already maintain auditing requirements established through HIPAA and the ARRA Health Information Technology for Economic and Clinical Health Act (HITECH Act). These regulations require providers to monitor every access, use and change to a patient record. Because the statewide HIE is primarily decentralized, and involved only in the exchange of health information from one authorized user to another, the statewide HIE audit logs will only contain information such as: 1) provider log-in identification; 2) provider name; 3) provider organization; 4) date and time; 5) patient account that was accessed; 6) type of records viewed by the provider; and 7) all failed log-ins. The providers' auditing processes will be able to provide detailed audit logs about additional events, such as specific updates or corrections made to a patient record, or individuals within the organization that viewed or modified a patient record.

In general, the statewide HIE will be able to show the organizations that have accessed an individual's health information through the statewide HIE. Additional information about how a record may have been used or modified will be available directly through the provider organization.

*A workflow diagram is being developed to illustrate the process for requesting audit logs from the statewide HIE or from the provider.*



*Proposed Policies:*

1. The statewide HIE and all participants will maintain audit logs pursuant to regulatory guidelines that document individuals accessing patient health information through the statewide HIE. The audit logs shall minimally identify: 1) participant log-in identification; 2) participant name; 3) participant organization; 4) date and time; 5) patient account that was accessed; 6) type of records viewed by the participant; and 7) all failed log-ins.
2. The statewide HIE will determine audit requirements, including: 1) the data elements to be maintained for auditing participant access to patient health information; 2) the expectations for participants to submit audit data to the statewide HIE; and 3) the minimum retention time of audit logs maintained for auditing participant access to patient health information. All participants will comply with audit requirements as specified by the statewide HIE.
  - Data Elements: To be determined with the HIE vendor
  - Processes to submit audit data: To be determined with the HIE vendor
  - Retention time of audit logs: To be determined with the HIE vendor
3. The statewide HIE and participants must review generated audit logs of HIE activity on a regular basis. Unusual activity and possible violations must be documented and appropriate mitigating action must be taken and documented, which are minimally consistent with the provisions of the HIPAA security rule.
  - Periodic technical and non-technical evaluations are required to ensure that the participants are compliant with the provisions of the HIPAA security rule and the statewide HIE privacy and security policies. Internal compliance audits shall be performed at least annually and when any major system or business changes occur. External compliance audits shall be performed at least [how often and when what].
4. The statewide HIE will develop procedures for responding to possible violations. Participants will comply with procedures for responding to possible violations.
  - Participants and the statewide HIE shall cooperatively investigate situations where patient health information may have been inappropriately accessed.
  - Employees and business associates of the participant shall report possible breaches of confidentiality to the participant's Security and/or Privacy Officer.
  - Participants shall alert the statewide HIE, other participants, and patients (when required by law) of situations where patient health information may have been inappropriately accessed.
  - Notification guidelines include:
    - The name of any persons involved with the possible violation shall be reported to the statewide HIE within the timeline required by HITECH and State Code Chapter 715C "Personal Information Security Breach Protection".
      - Timeline<sup>3</sup>: Without unreasonable delay and in no case later than 60 days following a breach
    - A record of the event and any discipline imposed shall be maintained by the participant, and be provided to the statewide HIE within the timeline required by HITECH
    - The participant is responsible for determining the severity of sanctions necessary, in accordance with the participant's policies and procedures. A record of the final determination shall be maintained by the participant, and be provided to the statewide HIE within the timeline required by HITECH.
      - Timeline: Without unreasonable delay and in no case later than 60 days following a breach
    - Any additional reports related to the possible violation shall be provided to the statewide HIE within 60 days of discovery.
  - All participants must provide to the statewide HIE within 30 days of submission to the Office of Civil Rights (OCR) a copy of the Federal Audit Report for Security and

---

<sup>3</sup> U.S. Department of Health and Human Services, "HITECH Breach Notification Interim Final Rule."  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html> (accessed 9/9/10)



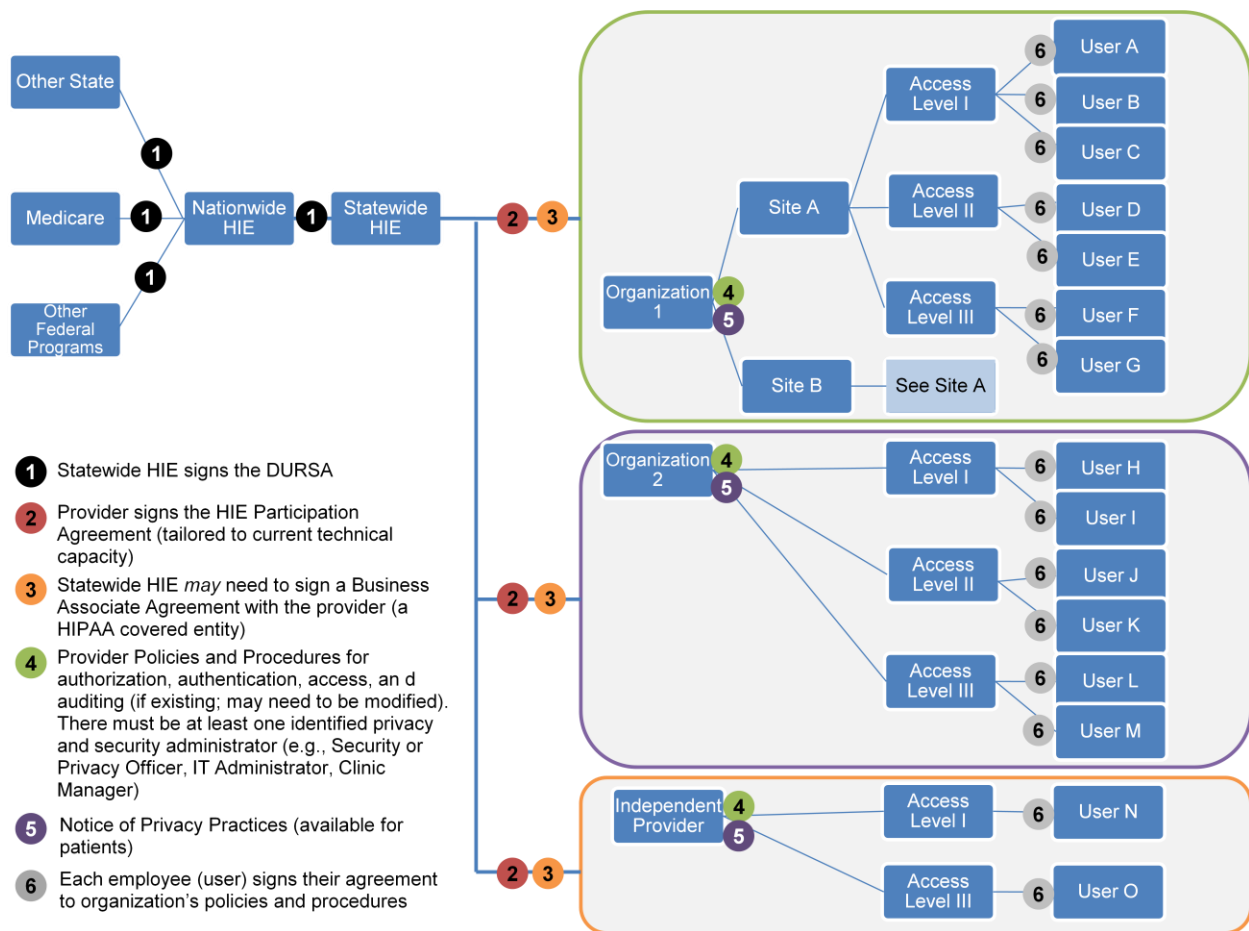
Privacy Breaches required to be submitted annually through the U.S. Department of Health and Human Services to OCR.

## Participation agreements

All organizational participants and independent participants shall sign a statewide HIE participation agreement which defines the privacy and security obligations of the parties participating in the statewide HIE.

Data sharing and participant agreements (i.e., HIE Participation Agreement) establish common agreement on essential policies to address compliance with applicable law, cooperation with other HIE participants, expectations to use the statewide HIE only for permitted purposes, limitation on the future use of data received through the statewide HIE, and privacy and security measures required to be in place before using the statewide HIE.

The following diagram illustrates the various trust agreements that will be necessary:



At the national level, a Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that must be signed by Iowa e-Health in order to exchange data with other exchanges through the Nationwide Health Information Network (NHIN). A similar agreement must be signed by all Iowa participants that want to use the statewide HIE. This agreement may require the participants to modify existing policies and procedures in areas such as authorization, authentication, access, and auditing and may add additional expectations related to privacy and security education and training for providers and



notification of HIE participation to patients. Participants must ensure that each user of the statewide HIE has agreed to the new or revised policies and procedures in order to access the statewide HIE.

The Department of Health and Human Services (DHHS) issued a notice of proposed rulemaking (NPRM) on July 14, 2010 to make Modifications to the HIPAA Privacy, Security, and Enforcement Rules as a result of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Based on information in the NPRM related to Section 13408 of the HITECH Act, the statewide HIE will be considered a business associate of all HIPAA-covered participants. This will likely require a business associate agreement between each participating organization and the statewide HIE. The final rule is expected to be established by October 2010.

*Proposed Policies:*

1. The statewide HIE shall have a Data Use and Reciprocal Support Agreement (DURSA) with the Nationwide Health Information Network.
2. All participants interested in using the statewide HIE will need to sign and return the agreement to the Office of Health IT for review and approval. The statewide HIE participation agreement will define the privacy and security obligations of the parties participating in the statewide HIE and minimally include: 1) authorization of participants for data access; 2) permitted purposes for information access; 3) purposes NOT allowed; 4) authentication of participants; 5) procedures for enforcing compliance with agreements; 6) indemnification; 7) security breach reporting requirements; and 8) conflict resolution among HIE participants
3. All participants shall modify written privacy and security policies and procedures to be minimally compliant with all statewide HIE policies and procedures defined in the statewide HIE participation agreement.
  - o All participants shall establish processes for educating personnel about the policies and procedures of the statewide HIE.
  - o Participants must have policies and procedures for disciplining, restricting, or terminating employees who violate the policies and procedures of the statewide HIE.
  - o All participants shall develop and accept legally compliant sanction policies for addressing violations of policies and procedures of the statewide HIE.
  - o All participants shall maintain a process for authorized personnel to agree to the participant's privacy and security policies and procedures
4. All participants shall maintain a notice of privacy practices for patients. This notice shall minimally indicate that the participant shares information with the statewide HIE unless a patient chooses to opt-out of the statewide health information exchange.

*The HIE participation agreement is currently under development and not yet available.*

## Individual Choice to Participate in the Statewide HIE

Patients can opt-out of the statewide HIE. When a patient opts-out, the statewide HIE will maintain a record of the patient and their opt-out decision in its master patient index. The statewide HIE will not facilitate the exchange of health information to any requesting providers through its record locator service. Patients may choose to opt-back-in to the statewide HIE at any time.

There are generally three approaches to consent policies. These include:

- **No Consent:** Patient's health information is automatically placed into the statewide HIE, without any additional consent above and beyond consent already required and provided through HIPAA. This alternative assumes that all health information will be available to the system.
- **Opt Out:** Patient's health information is automatically placed into the statewide HIE and exchange is allowed for sharing health information without additional consent provided by the patient. The patient's information remains available for electronic exchange until the patient chooses to opt out of participation in the statewide HIE and revokes permissions. This alternative assumes more information will be available to the system.



- **Opt In:** Patient's health information is placed into the statewide HIE after the patient provides permission. Exchange of health information is not allowed without prior permission provided by the patient. This alternative assumes less information will be available to the system.

In Iowa, patients will have the opportunity to opt-out of participating in the statewide HIE. The vast majority of operational HIEs nationwide (e.g., Nebraska, Utah, Maryland, New Mexico, Maine, New Jersey, Tennessee, Delaware, California<sup>4</sup>) include all patients in the regional or statewide HIE unless they have "opted-out" of the HIE by signing a waiver form. The opt-out approach is a critical success factor for new statewide HIEs, because it allows the master patient index to be quickly populated and provides an opportunity for important patient information to be available to providers prior to a patient's visit or in an emergency situation. The opt-out patient consent policy demonstrates early value of the statewide HIE to providers and patients. For example, when a patient's clinical care summary (e.g., continuity of care document) is made available to the statewide HIE, an emergency room provider can quickly access an unconscious patient's allergies or other preexisting conditions. Access to this information helps the emergency room provider make the best care delivery decisions.

The statewide HIE will facilitate the transfer of health information between care providers. It is not a central data repository where all patient records are held. In this type of de-centralized data storage environment where the statewide HIE functions as a message delivery service, it is not the statewide HIE's role to remove or restrict access to specific data elements within a patient document traveling through the statewide HIE. If a document is made available to the statewide HIE, any provider with a treatment relationship with the patient may have access to that record.

It is important to note that the purpose of the statewide HIE is to improve quality of care and assure patient safety. To help providers provide the best possible care and to help ensure patient safety, providers must have access to complete information about the patient, including but not limited to, all current medications, diagnoses, and other providers interacting with the patient. If a patient has a concern about another provider viewing the information available through the statewide HIE (e.g., clinical care summary, medication history), then that patient may choose to opt-out. However, this decision could have a negative impact on quality of care and patient safety to the individual opting-out.

#### *Proposed Policies:*

1. Personal identifiers (e.g., name, address, birth date) necessary to match individual patients throughout Iowa health care delivery networks shall be maintained in a secure, master patient index managed by the statewide HIE.
2. Patients may decide to opt-out of the statewide HIE. When a patient opts-out, the statewide HIE will maintain record of the patient and their opt-out decision in its master patient index.
3. Patients may choose to opt-back-in to the statewide HIE at any time
4. The statewide HIE shall adopt procedures to receive and execute opt-out and opt-back-in instructions from HIE participants and patients.
5. All participants shall implement appropriate procedures to: 1) inform patients that the organization uses the statewide HIE; 2) inform patients of the purpose and benefit of participating in the statewide HIE; and 3) inform patients of their right to opt-out of the statewide HIE.
6. Providers are prohibited from denying treatment to any patient because the patient has chosen to opt-out of the statewide HIE. When a patient has decided to opt-out, the participant maintains the right and option to contact the patient's other providers for patient information through other authorized means (e.g., telephone, fax) as it relates to Treatment, Payment and Healthcare Operations (TPO) in accordance with HIPAA guidelines.

#### *Proposed Procedures to Opt-Out*

- Patients will be informed about the statewide HIE and their right to opt out in the following ways:
  - o Broad Iowa e-Health communication and outreach plan
  - o Brochures and opt-out forms will be available in the provider offices.

---

<sup>4</sup> National Academy of State Health Policy. <http://www.nashp.org/hit-privacy> (accessed 9/9/10)



- *Optional:* Providers may choose to send a postcard or letter to all patients 30-60 days prior to “go-live” with the statewide HIE
- A patient can opt-out in two ways: 1) through the statewide HIE, and 2) through the provider
  - Through the statewide HIE by: a) filling out a form online; b) calling Iowa e-Health to request an opt-out form that can be sent to the statewide HIE; and c) downloading and mailing an opt-out form directly to the statewide HIE. The statewide HIE will then note the patient preference through HIE administrator tools
  - Through their provider by filling out a form at the provider office; the provider will then note the patient preference through their direct connection or web-based portal connected to the statewide HIE
  - If recorded patient consent conflicts, the most recent date will prevail
- A patient can opt-back-in to the statewide HIE in the following ways:
  - Through the statewide HIE by: a) filling out a form online; b) calling Iowa e-Health to request a reinstatement form that can be sent to the statewide HIE; and c) downloading and mailing a reinstatement form directly to the statewide HIE
- A provider will know if a patient has decided to opt-out by:
  - Receiving a message after they successfully match their patient through the MPI, but before the RLS queries for any documents
  - If a patient has submitted their decision to opt-out at one provider location, they will be opted-out at all other provider locations unless they submit a form to the statewide HIE requesting to reinstate their participation (i.e., opt-back-in)

*A workflow diagram is being developed to describe the process for consumers to opt-out. The opt-out form is also under development and not yet available.*

## Disclosure limitation

Health information will be shared with providers who have a treatment related reason to view the patient information. The provider may use the statewide HIE to report health information that is required by law. De-identified data may be available to population health and research entities, but the statewide HIE will not sell or disclose patient information.

### *Proposed Policies:*

1. No participant of the statewide HIE may release or publish individually indentifying health information exchanged through the statewide HIE for purposes unrelated to the treatment or billing of the patient who is the subject of the information.
2. Where identifiable information is required to be reported by law, the provider may use the statewide HIE to report the information to the statewide HIE even if the patient has opted-out.
3. Use or distribution of the information for a marketing purpose is strictly prohibited.
4. Secure, role-based access shall mitigate the potential for authorized participants to access information inappropriate for their defined roles in the participating organization and the statewide HIE.
5. De-identified data from the statewide HIE may be made available to authorized population health and research entities.



## Compliance with Health Insurance Portability and Accountability Act of 1996

All information maintained and exchanged through the statewide HIE is minimally covered by the policies, procedures, and regulations established by HIPAA and HITECH.

### *Proposed Policies:*

1. All participants providing information to the statewide HIE shall retain a property right in that information, but grant to participants of the statewide HIE a nonexclusive license to retrieve and use that information in accordance with HIPAA and any amendments and regulations under the act, state confidentiality laws and the policies procedures and rules established by the board.
2. Iowa e-health and all participants using the statewide HIE are responsible for following breach notification policies as defined by Health Insurance Portability and accountability Act of 1996 and any amendments and regulations under the act and the health information technology for clinical and economic health act. Participants must meet all HIPAA and HITECH requirements. This includes but is not limited to:
  - Protected Health Information in Paper or Oral Form:
    - The statewide HIE does not make use of information on these forms and places no further restrictions on the use of such information beyond already established participant policies and procedures.
  - Protected Health Information in Electronic Form:
    - Participants must ensure that access devices are equipped with reasonable and appropriate security measures so that unauthorized persons cannot access the statewide HIE.
    - Participants must restrict access to the statewide HIE to personnel who have a legitimate and identified need to have such access, and who have been granted such access in accordance with the statewide HIE policies and procedures for Authentication, Access, and Authorization for the administrative, technical, physical safeguards as outlined in the HIPAA security rule
  - Breach notification
    - Participants and the statewide HIE are individually responsible for following breach notification policies as defined by HIPAA and HITECH
  - Accounting of disclosure
    - Participants are responsible for disclosure of information as requested by patients.
    - Participants may request from the statewide HIE on behalf of the patient a history of the exchange that occurred.

## Openness and transparency

*There will be openness and transparency about policies, procedures, and technologies that directly affect patients and/or their electronic health information.*

Trust in electronic exchange of health information can best be established in an open and transparent environment. To protect the privacy of patients (or consumers) and to maintain a patient-centered solution, policies must be established to ensure the accuracy and confidentiality of information available and exchanged through the statewide HIE. Additionally, patients must be able to understand that electronic health information exists, how that health information is collected, used, and disclosed, and how they can exercise choice over participating in the statewide HIE.

The statewide HIE will most likely be considered a business associate of all HIPAA covered entities (pending the final rule from the July 14, 2010 NPRM on Modifications to the HIPAA Privacy, Security, and Enforcement Rules). As a business associate, the statewide HIE will be required to comply with HIPAA audit and logging requirements. In a decentralized data storage environment where the statewide HIE facilitates the exchange of information among providers, rather than storing actual patient records, the level of detail maintained in the audit records will be different than the audit records maintained by the provider organization (the HIPAA covered entity). See the [Audit](#) section for more information.



As the statewide HIE matures, Iowa e-Health plans to implement a patient portal (target date to be determined with the HIE vendor). Through the portal, patients will be able to set up an account with the statewide HIE and access the same documents available to their providers (e.g., a CCD or immunization history). Until the patient portal functionality is available, patients may access their health information through their provider or health care organizations. Some provider organizations are in the process of implementing patient portals through their EHR system to share this information with patients, while other provider organizations may make this information available through other means which will allow the patient to save or upload information into a personal health record. The patient portal may also include instructions for patients on how to contact their provider if they notice an error in one of their records.

*Proposed Policies:*

1. Process to receive notification of a violation of the confidentiality provisions required under this section;
2. Process to view an audit report created under this section for the purpose of monitoring access to the patient's records.

## Monitoring of usage and enforcement of HIE policies

Once privacy and security policies have been established to ensure the accuracy and confidentiality of information available through the statewide HIE, it is imperative to monitor compliance with the policies to build and maintain the integrity and trust of the statewide HIE. All participants accessing or using the statewide HIE must know that failure to comply with policies will result in penalties.

Any state law related to Iowa e-Health can be enforced by the Attorney General's Office, which also has authority under the new privacy regulations in ARRA to monitor data security for medical records. The Attorney General's Office, the Iowa e-Health governing body, and the IDPH Office of Health IT will provide oversight functions related to privacy and security compliance.

*Proposed Policies:*

1. Establish compliance roles of the department and office of the attorney general;
2. Provide the ability to issue warnings, write citations, and collect fines for noncompliance;
3. Establish penalties for violation.

## Limitation of Liability/Immunity

The purpose of the statewide HIE is to encourage the electronic exchange of health information among providers, which will support patient safety and continuity of care among a patient's providers. To provide a safe harbor for providers that are participating in the statewide HIE in good-faith and with authorization to do so, providers will not be liable solely based on their decision to use (or not use) information available through the statewide HIE.

*Proposed Policies:*

1. No participant who, in good in good faith, participates in the statewide HIE shall be liable in any action for damages or costs of any nature, in law or equity, which result solely from that participant's use or failure to use network information or data that was sent or retrieved in accordance with any amendments and regulations under the act, state, confidentiality laws and the rules, policies and procedures of the statewide HIE as approved by the board.

## Reconciliation with Other laws

HIPAA, other federal laws, and/or state law recognize HIV/AIDS, mental health, substance abuse, genetics information, etc. to be sensitive types of health information that warrant heightened scrutiny and privacy and security protections. State and federal laws have been developed to address patient concern



that information regarding these types of treatment will: 1) be accessed by health plans and employers, for example, to deny insurance coverage or job promotions; 2) be “hacked into” and shared inappropriately, causing social ostracizing or personal embarrassment; 3) be “tracked” or “watched” by the government; or 4) in general, fall into the wrong hands and violate personal privacy.

In Iowa, state law<sup>5</sup> provides heightened security above HIPAA regulations to protect sensitive patient information related to HIV/AIDS and mental health. These regulations limit the exchange of important patient information for treatment related purposes. The inability to share such information, even among a patient’s regular care providers, can impact treatment decisions and compromise patient safety (e.g., providers may not have record of medications prescribed to the patient). Ambiguity, complexity, and different interpretations of the laws and provisions often result in the impression that it is safer for providers (from a liability perspective) to not disclose any patient information. Furthermore, any regulations above and beyond HIPAA will hinder inter-state data exchange, which is imperative to provide full continuity of care among a patient’s various providers.

To promote patient safety and to provide a safe harbor for providers that are participating in the statewide HIE in good-faith and with authorization to do so, Iowa e-Health is seeking statutory language that would allow the exchange of health information for treatment-related purposes without additional consent above and beyond HIPAA.

Rather than modifying language in each code chapter, a pre-emption or alternate provision approach can be taken to exempt providers from specific laws or provisions. This statutory language would only be applicable to electronic information exchange. Paper-based health information exchanges would follow all current rules. Some examples of similar pre-emption or alternate provisions include:

- Iowa drug testing statute (Iowa Code 730.5) – An individual is subject to the statute unless he or she is testing for a commercial driver’s license where the individual is subject to U.S. Department of Transportation regulations and testing lists (49 CFR Part 383).

This exemption will:

- NOT lift restrictions on sharing information for non-treatment related purposes [e.g., an ER doctor can use the statewide HIE to learn that a patient has HIV, but that information would not be available to an insurance company by the statewide HIE]
- Help support provider adoption of the statewide HIE (i.e., by participating in the statewide HIE they will be safe from provisions considered to be “hidden traps” that would otherwise keep them from disclosing patient information)
- Help support inter-state data exchange (i.e., any patient consent laws above and beyond HIPAA will make inter-state data exchange much more difficult to achieve and may hinder a patient’s ability to receive continuity of care within Iowa as well as other states)

*Proposed Policies:*

1. Notwithstanding chapter 22, the following records shall be kept confidential, unless otherwise ordered by a court, with the patient’s consent, or by a person duly authorized to release such information: The identified and de-identified health information in the form of health data or medical records contained in, stored in, submitted to, transferred or exchanged by, or released from the statewide HIE, and identified and de-identified health information in the form of health data or medical records in the possession of Iowa e-health due to its administration of the statewide HIE. The terms “identified” and “de-identified” shall have the same meaning as in HIPAA.
2. When using the statewide HIE for the purposes of patient treatment, a participant is exempt from any other Iowa law that is more restrictive than the Health Insurance Portability and Accountability Act of 1996 which would otherwise prevent or hinder the exchange of patient information among a patient’s providers.

---

<sup>5</sup> Iowa Code Section 141A (HIV/AIDS) and Iowa Code Chapters 228 and 229 (Mental Health)



## Contact Information and Procedures

- A participant who has any questions regarding these statewide HIE policies and procedures shall first contact their supervisor or the Security and/or Privacy Officer of their organization. If necessary, the supervisor or the Security and/or Privacy Officer of the organizational participant (i.e., provider practice, hospital, public health, payers) will contact (or direct the participant to contact) Iowa e-Health directly at (866) 924-4636 or [ehealth@idph.state.ia.us](mailto:ehealth@idph.state.ia.us).
- If patients have any questions regarding these statewide HIE policies and procedures, they are encouraged to first contact their provider who is participating in the statewide HIE. Alternatively, patients may contact Iowa e-Health at (866) 924-4636 or [ehealth@idph.state.ia.us](mailto:ehealth@idph.state.ia.us).

## Frequently Asked Questions

*To be developed*