

## GENERAL PRINCIPLES FOR AUTHORIZING AND AUTHENTICATING INDIVIDUALS, SETTING ACCESS CONTROLS, AND AUDITING IN A HEALTH INFORMATION EXCHANGE

---

### OVERVIEW OF AUTHORIZATION, AUTHENTICATION, ACCESS CONTROL, AND AUDITING ISSUES

---

The second overarching privacy and security issue that must be solved to advance the automated, real-time electronic exchange of health information is the development of a framework for addressing four interrelated security topics:

- Mechanisms to establish and maintain a list of individuals authorized to access patient data;
- Methods to authenticate authorized individuals who access patient data;
- Information access controls – within information systems and through coordinated organizational policies – to limit authorized individuals' access to the patient data that is appropriate for the individual's functions and needs; and
- Mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.

The first issue facing organizations in a health information exchange is determining who should be authorized to access their organization's electronic health records. The task of managing the list of authorized individuals across organizations is difficult as the organizations' staff changes. Organizations need mechanisms to quickly exchange information and to use the information to add and remove authorized users in a timely fashion. This task becomes increasingly difficult as the number of organizations and authorized individuals increases.

The second issue facing organizations in a health information exchange is how authorized, external users will be authenticated when accessing health records. Current authentication methods (e.g., passwords and security fobs) create a secure system. However, the system can be cumbersome to use, because individuals may have multiple user IDs and passwords that change frequently. As the number of organizations allowing health care providers access to their electronic health record increases, so does the number of user IDs, passwords, and security fobs. The need to manage these security measures places a burden on the individual health care provider that acts as a barrier to accessing patient information.

The third issue facing organizations in a health information exchange is how to set access controls to appropriately restrict authorized individuals' access to patient data. Limitations in information systems require organizations to control access through organizational policies and behavioral controls. However, achieving compliance with the policies requires organizations to have a coordinated approach to activities that have traditionally not been synchronized across different organizations. At a minimum, organizations need a common approach to:

- Conducting training programs that assist employees in understanding and applying the policies;
- Deploying mechanisms to monitor and audit employees' compliance with the policies; and
- Setting sanctions for disciplining employees who violate the policies.

The fourth issue facing organizations in a health information exchange is the need to develop mechanisms for coordinated auditing of individuals' access to health information across organizations. Auditing individuals' access to patients' health information is critical to protecting the privacy and confidentiality of health information. When an external individual accesses an organization's electronic health records, the organization does not usually have the information necessary to determine if the access is legitimate and must rely on other organizations within the health information exchange to share information so that the determination can be made. Therefore, significant collaboration and coordination must occur between organizations in a health information exchange for auditing to be effective in protecting the privacy and confidentiality of health information.

---

### **GENERAL PRINCIPLES FOR AUTHORIZING AND AUTHENTICATING INDIVIDUALS, SETTING ACCESS CONTROLS, AND AUDITING IN A HEALTH INFORMATION EXCHANGE**

---

Specific solutions to the issues identified as authorization, authentication, access control, and auditing issues will depend on a number of factors beyond the control of this project. For example, the architecture of a health information exchange, the information technologies used by health care organizations, the standards currently being developed in national efforts, and health care organizations' experience in exchanging information will all significantly influence the framework and mechanisms used to address these issues.

To provide Minnesota health care organizations a foundation and framework for the continued development of health information exchanges, the 4A Subgroup identified a number of general principles that can guide organizations' decision making in forming and implementing health information exchanges. The general principles form a "conceptual solution" that was developed to be:

- independent of a health information exchange's architecture
- flexible enough to adapt to changes in information technology
- consistent with national standards currently under development
- capable of being refined and more finely detailed as health care organizations gain experience in implementing electronic health information exchange

The 4A Subgroup made five general assumptions regarding health information exchanges as part of their discussion and analysis of these issues. The Subgroup also identified nineteen general principles that health care organizations and health information exchanges should address as part of implementing an exchange. In addition to identifying the general principles, the Subgroup provided:

- discussion, analysis, and rationale for each principle
- recommended resources that may be useful for the further refinement and development of the principles to address changes and/or greater clarity in the architecture of a health information exchanges, information technologies, standards under development, and health care organizations' experience
- recommended expertise needed for the further refinement and development of the principles to address changes and/or greater clarity in the architecture of a health information exchanges, information technologies, standards under development, and health care organizations' experience

The report first presents all of the assumptions and principles without discussion and then presents an expand discussion and analysis of each of the principles:

**Assumptions**

- A.1** A Health Information Exchange will require all participants to sign a standard participation agreement. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each party. The signing of this agreement means that each participant will adhere to the policies and procedures of the Health Information Exchange.
- A.2** Health Information Exchanges will define the type of patient health information to be exchanged or accessed between organizations participating in a Health Information Exchange.
- A.3** Health Information Exchanges will exchange patients' health information using national standards for data content and data definitions.
- A.4** The exchange of patient health information through a health information exchange will occur using standard-based messaging and/or view-only access to provider's electronic health records.
- A.5** All organizations participating in a Health Information Exchange will have adopted and implemented generally accepted security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of patients' health information.

**Authorization Principles**

- P1.1** All individuals having access to patients' health information through a Health Information Exchange will be assigned a unique ID for accessing the health information. Consistent with the authentication principles, each ID for accessing patients' health information shall require at least single-factor authentication (e.g., password) to access health information.
- P1.2** When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.
- P1.3** The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.
- P1.4** All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role-based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.
- P1.5** Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in a Health Information Exchange when the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

**Authentication Principles**

- P2.1** All organizations participating in a Health Information Exchange should minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.

- P2.2** All organizations participating in a Health Information Exchange should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the Health Information Exchange (i.e., across participating organizations).
- P2.3** Authentication of individuals accessing patients' health information through a Health Information Exchange should be as seamless as possible when accessing information across participating organizations.
- P2.4** From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through a Health Information Exchange should be the same process regardless of which participating organization's health information is being accessed.

### **Access Control Principles**

- P3.1** Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.
- P3.2** All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the Health Information Exchange.
- P3.3** All organizations participating in a Health Information Exchange should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing/exchanging patients' health information through a Health Information Exchange.
- P3.4** All organizations participating in a Health Information Exchange should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing/exchanging patients' health information through the Health Information Exchange.
- P3.5** Health Information Exchanges should define appropriate access to patients' health information and should develop policies and procedures for disabling individuals' access to patients' health information through a Health Information Exchange for inappropriately accessing patients' health information.
- P3.6** Health Information Exchanges should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.

### **Auditing Principles**

- P4.1** All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.
- P4.2** All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.
- P4.3** All organizations participating in a Health Information Exchange should develop and accept: a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information; b) the frequency at which the auditing data will be exchanged between

organizations participating in the Health Information Exchange; and c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information.

- P4.4** All organizations participating in a Health Information Exchange should develop and accept procedures for: a) alerting other participating organizations of situations where patients' health information may have been inappropriately accessed; and b) jointly investigating situations where patients' health information may have been inappropriately accessed.

---

## EXPANDED DISCUSSION AND ANALYSIS OF GENERAL PRINCIPLES

---

The 4A Subgroup's discussion and analysis of the general principles for authorizing and authenticating individuals, setting access controls, and auditing in a health information exchange was done assuming that the following assumptions are true:

- A.1** A Health Information Exchange will require all participants to sign a standard participation agreement. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each party. The signing of this agreement means that each participant will adhere to the policies and procedures of the Health Information Exchange.
- A.2** Health Information Exchanges will define the type of patient health information to be exchanged or accessed between organizations participating in a Health Information Exchange.
- A.3** Health Information Exchanges will exchange patients' health information using national standards for data content and data definitions.
- A.4** The exchange of patient health information through a health information exchange will occur using standard-based messaging and/or view-only access to provider's electronic health records.
- A.5** All organizations participating in a Health Information Exchange will have adopted and implemented generally accepted security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of patients' health information.

### **Authorization Principle P1.1:**

**All individuals having access to patients' health information through a Health Information Exchange will be assigned a unique ID for accessing the health information. Consistent with the authentication principles, each ID for accessing patients' health information shall require at least single-factor authentication (e.g., password) to access health information.**

#### **Discussion and Analysis:**

This principle is an adaptation of the HIPAA Security regulation requirement that all individuals granted access to electronic protected health information be assigned a unique name and/or number for identifying and tracking users' identity (45 CFR 164.312(a)(2)(i)). This principle also incorporates the HIPAA Security regulation requirement that organizations implement procedures to authenticate/verify that an individual seeking access to electronic protected health information is who they claim (45 CFR 164.312(d)). This principle allows organizations and health information exchanges to create audit logs that monitor and track individuals' access and use of patients' health information.

The 4A Subgroup also recommends that the unique ID not have any other required characteristics beyond being unique across organizations. For example, the unique ID should not contain embedded intelligence, such as user or organization name or location.

The 4A Subgroup believes that this principle represents the standard practice within health care organizations and does not need additional development

#### **Authorization Principle P1.2:**

**When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.**

#### **Discussion and Analysis:**

This principle assigns organizational responsibility for all individuals that access patients' health information through a health information exchange. An individual is granted access to patients' health information because at least one organization participating in the health information exchange has determined that the individual needs the access for their job functions.

This principle identifies three required activities for organizations that grant individuals access to patient health information through a health information exchange:

- Authorize the individual – The organization should conduct those activities needed to authorize the individual, such as verifying identity, setting role-based access, and providing authentication information and tools.
- Maintain appropriate access – The organization should maintain individuals' access consistent with their roles and job functions. Hence, if an individual changes roles or job functions, it is the responsibility of the authorizing organization to ensure that those changes are communicated to the health information exchange. This means that organizations may need to perform periodic reviews of individuals' access to the health information exchange to properly maintain individuals' access to health information.
- Terminate access – When it is no longer appropriate for an individual to have access to patients' health information the authorizing organization should terminate that access to the health information exchange.

A health care provider working at multiple organizations participating in a health information exchange may be authorized by more than one organization. However, at least one of the organizations must take responsibility for ensuring appropriate access.

#### **Recommended Resources for Further Development:**

- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- The policies and procedures of other health information exchanges.

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- IT security professionals
- Health information managers

- Human resources
- Legal counsel

### **Authorization Principle P1.3:**

**The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.**

#### **Discussion and Analysis:**

This principle is based on the HIPAA Privacy regulations minimum necessary principle that requires organizations to make reasonable efforts to limit access/disclosures of protected health information to the minimum necessary for accomplishing the intended purpose of the use or disclosure. Most health care organizations currently use some type of role-based access to limit individuals' access to patients' health information. Unfortunately, organizations define their roles differently, so there is a need to create a common framework for role-based access when exchanging information through a health information exchange.

This principle does not require that all organizations use the same framework for role-based access within their organizations. Rather, the principle recommends developing an agreed upon set of roles for exchanging information between organizations through the health information exchange.

#### **Recommended Resources for Further Development:**

Health information exchanges that develop role-based access standards may find that the following national efforts useful in implementing a standard that is likely to be consistent with other health information exchanges:

- ISO/CD TS 21298, "*Health informatics -- Functional and structural roles*"
- ASTM E1986, "*Standard Guide for Information Access Privileges to Health Information*"
- Best practices and recommendations from professional organizations such as:
  - American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
  - Health Information Management Systems Society (HIMSS)

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- Health care providers and others that need access to patients' health information to accomplish their job functions
- Health information managers
- IT security and operations professionals
- Human resources

**Authorization Principle P1.4:**

All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role-based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.

**Discussion and Analysis:**

This principle identifies the minimum set of activities an organization needs to perform when authorizing an individual to access information through a health information exchange. The requirements of this principle are based on, and consistent with, other principles. For example, this principle recommends that an individual be granted an appropriate level of access to patients' health information through a health information exchange based on the role-based access standards developed in Principle 1.3.

This principle uses the term "security credentialing" to denote the activities needed to grant individuals access to health information through a health information exchange. The term was used to distinguish those activities from other credentialing that might be performed by health care organizations, such as medically credentialing a provider to practice medicine in a facility. The 4A Subgroup believes the security credentialing process needs to be as streamlined as possible. That is, the process should require those procedures and activities necessary to ensure that individuals' access is appropriate and secure, but should not contain other procedures not directly related to granting access to the health information exchange.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following state and national efforts useful in developing policies and procedures for security credentialing:

- o The experiences of other health information exchanges, such as the Community Health Information Collaborative (CHIC).
- o ISO/CD TS 21298, "*Health informatics -- Functional and structural roles*"
- o ISO/TS 21091:2005, "*Health informatics -- Directory services for security, communications and identification of professionals and patients*"

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in the development of the policies and procedures used to implement this principle:

- o IT security and operations professionals
- o Health information managers
- o Human resources

**Authorization Principle P1.5:**

**Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in a Health Information Exchange when the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.**

**Discussion and Analysis:**

This principle recommends maintaining the same level of medical credentialing requirements for exchanging patients' health information electronically that are currently used for paper records.

Medical credentialing are those activities needed to verify that a provider is appropriately qualified to practice medicine in a health care organization and includes activities such as verifying licensure and certifications. Medical credentialing is an expensive and time-consuming process. Currently, health care organizations exchange patients' health information without requiring that the requesting provider be medically credentialed by the disclosing provider. This principle recommends that simply accessing patients' health information, without the ability to change the record, should not require medical credentialing.

Some organizations' medical credentialing process is linked to their security credentialing process. That is, a provider who needs to be medically credentialed cannot be granted access to electronic health records prior to completing the medical credentialing process. Therefore, organizations may need to modify their processes to implement this principle. Some 4A Subgroup members believe that medical credentialing should be required if a provider has electronic access to all of an organization's electronic patient records. However, it is unclear how this level of credentialing yields greater security for the patients' health records than the security credentialing required in Principle 1.4.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following efforts useful in clarifying the requirements for medical credentialing:

- The medical credentialing requirements used by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
- The medical credentialing requirements for providers as part of their Medicare participation
- Integrating the Healthcare Enterprise's (IHE) work in developing a common framework to deliver the basic interoperability needed for local and regional health information networks. The work includes a security framework for protecting the confidentiality, authenticity and integrity of patient care data.

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Medical credentialing staff familiar with JCAHO and Medicare requirements
- IT security and operations professionals
- Health information managers

- Human resources

**Authentication Principle P2.1:**

**All organizations participating in a Health Information Exchange must minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.**

**Discussion and Analysis:**

This principle is a corollary to Principle P1.1 and is an adaptation of the HIPAA Security regulations requirement that organizations implement procedures to authenticate/verify that an individual seeking access to electronic protected health information is who they claim (45 CFR 164.312(d)).

The 4A Subgroup did not want to be more specific about the type of authentication that may be required and believed that any of the following three possible types factors could be appropriate:

- Something the individual knows, such as an ID and password or PIN.
- Something the individual has, such as, a security fob, smart card or other physical object that must be presented to enable access.
- Something the individual is, such as, a unique personal biometric (e.g., fingerprint or retina scan).

The 4A Subgroup believes that this principle represents the standard practice within health care organizations and does not need additional development

**Authentication Principle P2.2:**

**All organizations participating in a Health Information Exchange should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the Health Information Exchange (i.e., across participating organizations).**

**Discussion and Analysis:**

This principle recognizes health care organizations' interests in maintaining a heightened level of security when patients' health information is transmitted, accessed, or exchanged through external networks and connections. This principle is consistent with most health care organizations' current policies related to remote access of electronic health records, which generally require two-factor authentication. As indicated in Principle 2.1 there are many possible authentication mechanisms that could be used to implement this principle. The 4A Subgroup did not want to be more specific about the two authentication factors to ensure that organizations and health information exchanges have flexibility in implementing this principle.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following national efforts useful to help assure consistency with other health information exchanges as they implement this principle:

- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This

workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.

- The eHealth Initiative's and Foundation workgroups. The eHealth Initiative and the Foundation for eHealth Initiative are independent, non-profit affiliated organizations whose missions are to drive improvement in the quality, safety, and efficiency of healthcare through information and information technology.
- The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.
- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations professionals
- Health information managers
- Health care providers and others that need to access patients' health information to accomplish their job functions

**Authentication Principle P2.3:**

**Authentication of individuals accessing patients' health information through a Health Information Exchange should be as seamless as possible when accessing information across participating organizations.**

**Discussion and Analysis:**

This principle addresses the need to make the process of accessing patients' health information through a health information exchange as easy as possible to facilitate its use by providers. There is empirical evidence that providers are disinclined to search for and access patients' health information as the process for doing so becomes more cumbersome. Therefore, organizations and health information exchanges should try to identify provider authentication mechanisms and processes that fit into providers' work flow to maximize the potential of a health information exchange to improve patient care.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following national efforts useful to help assure consistency with other health information exchanges as they implement this principle:

- The experiences of other health information exchanges, such as the Community Health Information Collaborative (CHIC).
- Integrating the Healthcare Enterprise (IHE) and their IT Infrastructure Technical Framework

- The Liberty Alliance Project and their work on federated identity, which seeks to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information.
- ISO/TS 21091:2005, "*Health informatics -- Directory services for security, communications and identification of professionals and patients*"
- The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need to access patients' health information to accomplish their job functions
- IT security and operations professionals
- Health information managers

**Authentication Principle P2.4:**

**From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through a Health Information Exchange should be the same process regardless of which participating organization's health information is being accessed.**

**Discussion and Analysis:**

This principle extends Principle 2.3 by stating that the authentication process should look and act the same to the health care provider regardless of which participating organization's health information is being accessed. By using the same authentication process to access health information from all participating organizations it will be easier for providers to learn and remember the process. Thus, providers will be more likely to search for and access patients' health information from other sources.

The 4A Subgroup does not intend this principle to imply that the technical authentication processes used by organizations to authenticate each others' providers must be the same. The Subgroup recognized that the exact authentication mechanisms might depend on a number of technological issues. However, it is important to address those issues in a manner that causes the least amount of variation in health care providers' activities.

The Subgroup also noted that there may be a need to develop special authentication procedures for access to sensitive health information, such as mental health or substance abuse treatment. Even in these cases, the 4A Subgroup believes that it is important to minimize the variation in the activities required for a provider to access patients' health information.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following national efforts useful to help assure consistency with other health information exchanges as they implement this principle:

- The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) and their collaboration on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.
- ISO/TS 21091:2005, "*Health informatics -- Directory services for security, communications and identification of professionals and patients*"
- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E1762-95(2003), "*Standard Guide for Electronic Authentication of Health Care Information*"

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need to access patients' health information to accomplish their job functions
- IT security and operations professionals
- Health information managers
- Electronic health record vendors

**Access Control Principle P3.1:**

**Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.**

**Discussion and Analysis:**

This principle represents an idealized notion of when and how patients' health information should be accessed by health care providers. It is an idealized notion because it is impossible to know a priori what information may be relevant to the treatment of a patient. It is only after a patient has been diagnosed and treated that it is possible to know what health information was relevant to the treatment provided.

There are two types of access controls: 1) behavioral controls set by organizational policies; and 2) enforced information systems' controls. This principle is intended to serve as a behavioral control and guideline for health care providers' in deciding when and how they should access patients' health information. As with other behavior controls, this principle will only be achieved if there are clear policies, provider education, and sanctions developed to support the principle.

There are two reasons it would be impossible to implement this principle as an enforced information system control. First, health care providers have a constantly evolving and complex set of relationships with patients (e.g., treating relationship, consulting relationship with the treating provider etc.). It is not feasible or practical to try to maintain such a list of relationships. Second, it is impossible to know a priori what information may be relevant to the treatment of a patient and too stringently limiting health care providers' access to patients' health information can have a negative impact on patient care. Therefore, this principle is intended ensure that providers uphold their

professional responsibility to self-limit their access to patients' health information to the information needed to provide appropriate patient care.

To ensure that this principle does not inappropriately restrict a provider's access to necessary patient information, the 4A Subgroup believes that it is important to have a broad and inclusive definition of the term "Treatment Relationship." The Subgroup used the following adaptation of the HIPAA definition of treatment in its discussions: "Treatment Relationship" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

#### **Recommended Resources for Further Development:**

Health care organizations may find that the following national efforts useful in implementing this principle:

- ISO 26000, "*Guidance on social responsibility*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- ASTM E1988-98, "*Standard Guide for Training of Persons who have Access to Health Information*"
- ASTM E1986-98(2005), "*Standard Guide for Information Access Privileges to Health Information*"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.
- Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health care providers and others that need access to patients' health information to accomplish their job functions
- Training and development staff
- Chief Privacy Officer
- Corporate compliance staff
- Health information managers

**Access Control Principle P3.2:**

**All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the Health Information Exchange.**

**Discussion and Analysis:**

This principle addresses the need and importance of having explicit, written policies and procedures for accessing patients' health information through a health information exchange. As part of their HIPAA compliance activities, most health care organizations have developed and implemented written policies and procedures for electronically accessing health information within their organizations. This principle extends those policies and procedures to health information accessed through a health information exchange.

There are variations in health care organizations' policies and procedures for electronically accessing health information because of differences in organizations' implementation of health technology. It could be very difficult for all organizations participating in a health information exchange to adopt the same internal health information access policy. However, this principle envisions a common policy for accessing health information across organizations. The requirement for written policies and procedures is intended to ensure that there is a reference document that outlines the standards for accessing health information through a health information exchange. This reference document of written policies and procedures will also be helpful in implementing Principle 3.3 Training and Principle 3.4 Sanctions.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following national efforts useful in implementing this principle:

- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- ASTM E1986-98(2005), "*Standard Guide for Information Access Privileges to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.
- The eHealth Initiative's and Foundation workgroups. The eHealth Initiative and the Foundation for eHealth Initiative are independent, non-profit affiliated organizations whose missions are to drive improvement in the quality, safety, and efficiency of healthcare through information and information technology.
- Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Health information managers
- Legal counsel
- Human resources
- Chief Privacy Officers
- Corporate compliance staff

### **Access Control Principle P3.3:**

**All organizations participating in a Health Information Exchange should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing/exchanging patients' health information through a Health Information Exchange.**

#### **Discussion and Analysis:**

This principle highlights the importance of training and educating individuals about the policies and procedures for accessing patients' health information through a health information exchange. As noted in Principle 3.1, many of the access controls designed to protect patients' health information will be behavioral controls that require providers, and others, to take actions to access information appropriately. However, these behavioral controls will only be effective if: 1) the health information access policies and procedures developed under Principle 3.2 are clear; and 2) individuals understand the policies and procedures and their responsibilities within the procedures. Individuals will find it difficult to comply with policies and procedures that they do not understand. Hence, training will be critical to protecting the privacy of patients' health information.

#### **Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- ASTM E1988-98, "*Standard Guide for Training of Persons who have Access to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.
- Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)

#### **Recommended Experts for Further Development:**



Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Training and development staff
- Health information managers
- Human resources
- Corporate compliance staff

#### **Access Control Principle P3.4:**

**All organizations participating in a Health Information Exchange should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing/exchanging patients' health information through the Health Information Exchange.**

#### **Discussion and Analysis:**

This principle addresses situations where individuals violate organizations' policies and procedures for accessing patients' health information through a health information exchange. This principle has at least two components that will facilitate the electronic exchange of health information. First, many of the access controls that a health information exchanges utilizes will be behavioral controls. Under this principle, health care organizations and patients will have greater confidence in the effectiveness of those controls when there are consequences for violating the controls. Second, a common sanction policy across all organizations participating in a health information exchange will encourage a more uniform and equitable enforcement of the policies and procedures developed under Principle 3.2.

#### **Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- The Confidentiality, Privacy and Security Workgroup that is part of the US Department of Health and Human Services' American Health Information Community (AHIC). This workgroup is charged with making recommendations to AHIC regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Legal counsel
- Human resources

- Corporate compliance staff
- Health information managers
- Union representatives

**Access Control Principle P3.5:**

**Health Information Exchanges should define appropriate access to patients' health information and should develop policies and procedures for disabling individuals' access to patients' health information through a Health Information Exchange for inappropriately accessing patients' health information.**

**Discussion and Analysis:**

This principle identifies one mechanism that health information exchanges can use to protect patients' health information from being inappropriately accessed through a health information exchange. Implementing policies and procedures for disabling an individual's access to patients' health information through a health information exchange will require coordination with the organization responsible for authorizing the individual under Principle 1.2. Also, disabling a provider's access to patients' health information must be done in a manner that does not adversely impact patients' care.

**Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- ASTM E1986-98(2005), "*Standard Guide for Information Access Privileges to Health Information*"
- ASTM E1869-04, "*Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*"
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- The policies, procedures and experience of other health information exchanges, such as the Indiana Health Information Exchange (IHIE)
- ISO/TS 22600-1:2006, "*Health informatics -- Privilege management and access control -- Part 1: Overview and policy management*"

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- Legal counsel
- Corporate compliance staff
- Health information managers
- IT security and operations staff

- Health care providers and others that need access to patients' health information to accomplish their job functions

**Access Control Principle P3.6:**

**Health Information Exchanges should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.**

**Discussion and Analysis:**

This principle is an adaptation of the HIPAA Security regulation requirement that health care organizations implement procedures that terminate an electronic session after a predetermined time of inactivity (45 CFR 164.312(a)(2)(iii)). Most health care organizations have implemented this principle within their organizations, so this principle simply extends that implementation to health information exchanges. This principle will help to protect patients' health information by minimizing the possibility of information being inappropriately accessed through a computer that was left unattended.

This principle needs little additional development.

**Recommended Resources for Further Development:**

Health information exchanges may find that the following national efforts useful in implementing this principle:

- The policies, procedures and experience of other health information exchanges, such as the Indiana Health Information Exchange (IHIE)

**Recommended Stakeholders for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff

**Auditing Principle P4.1:**

**All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.**

**Discussion and Analysis:**

This principle addresses the first requirement of an auditing program – collecting sufficiently detailed data to facilitate an audit. This principle identifies the minimum data necessary to ensure that an organization can determine:

- Who accessed patients' health information
- What patient information was accessed
- When the patient information was accessed

Depending on the architecture of the health information exchange, it may be possible to log this data at either the organization level or at the health information exchange level. This principle does not specify where or how the data is logged and leaves that decision to the organizations and health information exchange. This principle focuses on what information needs to be collected and used as the foundation for the activities in Principles 4.2 and 4.3.

**Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers
- Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of the Minnesota Chapter of Information System Audit and Control Association and the Minnesota Chapter of the International Information Systems Forensics Association. These are the two leading professional organization focusing on information auditing and both have active Minnesota chapters. The Minnesota chapter of the Information System Audit and Control Association has an active Healthcare Security Professional Interest Group.

**Auditing Principle P4.2:**

**All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.**

**Discussion and Analysis:**

This principle identifies the auditing of individuals' access to patients' health information through a health information exchange as a significant tool for ensuring the patients' health information is not inappropriately accessed. As noted in the discussion of Principle 3.1, many of the access controls associated with a health information exchange will be behavioral controls. Therefore, an auditing

program is critical to verifying compliance with the controls developed to limit/prohibit inappropriate access to patients' health information.

Consumer acceptance and public trust will be crucial factors in the success of any health information exchange. This principle, in conjunction with related principles (e.g., Principle 4.4, Investigation of Inappropriate Access and Principle 3.4, Sanctions), will help to reassure patients that the health information is actively protecting their health information.

**Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- o Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- o ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- o Best practices and recommendations from trade organizations such as the American Health Information Management Association/Minnesota Health Information Management Association (AHIMA/MHIMA)
- o The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"

**Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- o IT security and operations staff
- o Health information managers
- o Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of the Minnesota Chapter of Information System Audit and Control Association and the Minnesota Chapter of the International Information Systems Forensics Association.

**Auditing Principle P4.3:**

**All organizations participating in a Health Information Exchange should develop and accept: a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information; b) the frequency at which the auditing data will be exchanged between organizations participating in the Health Information Exchange; and c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information.**

**Discussion and Analysis:**

This principle acknowledges that organizations participating in a health information exchange will need to share information in order to properly conduct routine audits as described in Principle 4.2. Although the exact information for auditing an organization would have available from its own sources would

depend on the architecture of the health information exchange, it is anticipated that organizations will need to share information to have the all the information needed for an audit. For example, the organization where a patient's health information has been accessed will have recorded:

- o who accessed the information
- o what information was accessed
- o when the information was accessed

However, that organization will not have the following necessary information:

- o whether or not the patient whose information was accessed being seen when the information was accessed
- o whether or not the provider accessing the patient's information was scheduled to work when the information was accessed
- o if the information that was accessed relevant to the current treatment of the patient
- o why the provider accessing the information may have had a need to access the information

All of these elements may be relevant and necessary to performing an audit. Additionally, this principle call for setting a minimum retention time of audit logs. This aspect of the principle is needed to account for the fact that individuals' inappropriate access of health information is often discovered during an investigation of a complaint, rather than through a routine audit. Therefore, this principle anticipates the need to maintain audit logs to facilitate complaint-based auditing.

#### **Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- o Research work at the National Committee on Vital and Health Statistics on the high level functional requirements for the national health information network.
- o ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- o Integrating the Healthcare Enterprise (IHE) and their work on audit trails and node authentication
- o The policies, procedures and experience of other health information exchanges

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- o IT security and operations staff
- o Health information managers
- o Corporate compliance staff

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of the Minnesota Chapter of Information System Audit and Control Association and the Minnesota Chapter of the International Information Systems Forensics Association.

#### **Auditing Principle P4.4:**

**All organizations participating in a Health Information Exchange should develop and accept procedures for: a) alerting other participating organizations of situations where patients' health information may have been inappropriately accessed; and b) jointly investigating situations where patients' health information may have been inappropriately accessed.**

#### **Discussion and Analysis:**

This principle describes the responsibility of organizations participating in a health information exchange to notify other participating organizations if there is evidence or concern that patients' health information may have been inappropriately accessed. There are a number of important reasons for developing procedures to alert other participating organizations of potentially inappropriate access:

- The organizations will be able to share specific information necessary for a complete investigation of the concern.
- All organizations have a responsibility to protect the confidentiality of their patients' data and should be alerted of any situation which may negatively impact their patients' privacy.
- Alerting other participating organizations of potential concerns will allow the organizations to identify, investigate, and mitigate systemic vulnerabilities related to the exchange of patients' health information.
- Alerting other participating organizations may help facilitate the implementation of Principles 3.4, Sanctions and Principle 3.5, Disabling Access.

#### **Recommended Resources for Further Development:**

Health care organizations and health information exchanges may find that the following national efforts useful in implementing this principle:

- ASTM E2147-01, "*Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*"
- The Markle Foundation's report titled, "*Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange.*"
- Integrating the Healthcare Enterprise (IHE) and their work on audit trails and node authentication
- The policies, procedures and experience of other health information exchanges

#### **Recommended Experts for Further Development:**

Organizations participating in a health information exchange will want or need the following areas of their organizations represented in implementing this principle:

- IT security and operations staff
- Health information managers

- Corporate compliance staff
- Legal counsel

Additionally, it would be beneficial to have professionals experienced in information technology audit issues such as, members of the Minnesota Chapter of Information System Audit and Control Association and the Minnesota Chapter of the International Information Systems Forensics Association.