

Minnesota Privacy and Security Project -- AAAA Work Group (Authorization, Authentication, Access Controls & Auditing) Meeting Notes – December 13, 2006

Attending:

Greg Jonsen, Co-Chair - HealthPartners, Greg Linden, Co-Chair – Stratis Health, Miaja Cassidy – Medica, Lee Olson – Mayo Clinic, Tom Reineke – Gillette Children's, Dan Routhe - University of Minnesota

On the Phone:

Diane Larson – St. Luke's, Tom Ihlenfeld – UCare, Melinda Machones – CHIC RHIO, Christina Stephans – University of Minnesota

Staff:

Mike DeWane – Rx2000 Institute, Jim Golden – Department of Health, Mike Thorsen – Rx2000 Institute, Christina Wen – Department of Health

1. Meeting Plan Objectives

Greg Jonsen called the meeting to order. Mike Thorsen reviewed the meeting objectives and work plan schedule. Mike stated that this meeting would focus on:

1. Review the updated Security Terms and Definitions
2. Review meeting notes from November 29th
3. Discussion of the expanded format for the Principles
4. Discussion of the three additional items (Discussion/analysis, Recommended resources & Recommended activity/action) under each Principle

Mike explained that sections for discussion/analysis points and recommendations under each Principle were added to the General Principles document. This discussion will focus on the two items of 'Possible resources for future activities' & 'Recommended stakeholder involvement' under each Principle.

2. Security Terms and Definitions Review

Mike Thorsen asked the group to review the updated Security Terms and Definitions especially the new terms which were added to the list. These new terms included:

***Computer Forensics** – The practice of gathering, retaining, and analyzing computer-related (audit) data for investigative purposes in a manner that maintains the integrity of the data. SOURCE: SP 800-61*

***Security Credentialing** – The process of reviewing and granting a user the appropriate role-based designation and access rights to specific health information.*

Treatment Relationship - *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. SOURCE: HIPAA*

Single-factor Authentication – *This is when only one of the three possible factor types is used to authenticate a person for system access. The three factor types are: 1. Something you know, such as an ID and password or PIN. 2. Something you have, such as, a security fob or smart card (a physical object that must be presented to enable access). 3. Something you are, such as, personal biometric (fingerprint, retina scan, etc.), which is unique.*

Mike also noted that we changed the Record Locator Service (RLS) definition so it matched the definition of the Patient Consent Group. The RLS definition now reads:

Record Locator Service (RLS) – *An electronic index of patient identifying (demographic) information that directs participants in a Health Information Exchange to the location of patient health information held providers as defined in section 144.335, subdivision 1 (b) and group purchasers as defined in section 62J.06, subdivision 6. SOURCE: Patient Consent/Liability subgroup*

Mike encouraged the group to continue to review this list and to send him edits, additions and deletions of any security terms and definitions before the next meeting

3. Efforts Beyond the AAAA Subgroup

Jim Golden led the group in a discussion about recommendation concerning ongoing efforts after the AAAA subgroup completes their work early next year. Jim acknowledged that there is no way to complete the assigned task in the short time allotted and he handed-out a one-page draft recommendation to identify group(s) that can continue this important work. Jim mentioned that the Minnesota Health Care Connection (MnHCC) and the Minnesota eHealth Advisory Committee (Technical Work Group) would be logical candidates to continue the work of the 4As group. MnHCC is in the process of creating a website that will address some of the 4As group's issue. Mike Thorsen mentioned the Healthcare Special Interest group of the local ISSA group as well as local and national chapters of HIMSS and AHIMA.

Greg Jonsen asked whether this recommendation would be submitted to RTI or to the eHealth Advisory Committee. Jim Golden reported that the recommendation will be submitted to both groups through the Final Report.

4. Discussion of the Expanded Format for the General Principles for Guidance in a Health Information Exchange

Mike Thorsen pointed out that of the three additional items have been added under each

General Principle for Guidance:

1. Discussion/analysis
2. Recommended resources
3. Recommended activity/action

Mike directed the group to the first Assumption in the Principles document to describe how these categories will be used:

Assumptions:

- ***A Health Information Exchange (HIE) 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 HIE.***

Discussion/analysis: Terms of the relationship and each participants roles, rights and responsibilities would have to be addressed in a HIE contract. The 4A group agreed that employers must assume full responsibility for authorizing their employees' access to healthcare information and also for terminating their employees' authorization. Thus, before encouraging the ubiquitous networking of patient health information, we must establish a common understanding and an adequate set of shared rules.

Possible resources for future activities: The Markle Foundation's suggested HIE contractual options as well as HIE operational agreements from other states; such as, Indiana are possible resources.

Recommended stakeholder involvement: Legal and health information experts representing hospitals, clinic, various health care providers and health plans plus legal and health information representatives of state government (MDH, MN DHS, U of MN, etc.) are all stakeholders.

Possible resources suggested were the Markle Foundation' sample contract and HIE contacts such as Indiana's. Recommended Stakeholders include provider and payer participants as well as legal and governmental agencies plus legal staff.

Jim Golden noted that all HIEs are naturally going to define a limited amount of information they will exchange. These judgments are typically based on improving patient care and economic feasibility. Jim also stated that we should identify all the logical national standards groups as possible resources for future activities. Jim also wanted the 4As work group to note which principles need further development and he gave several brief examples of how the group might approach this.

5. Discussion of General Principles for Guidance in a Health Information Exchange

Greg Linden directed the discussion concerning the *General Principles for Authorizing and Authenticating Individuals, Setting Access Controls and Auditing in a Health Information Exchange*. The discussion began with authorization.

AUTHORIZATION

P1 -- All individuals having access to patients' health information through an HIE 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/analysis: **New** -- This is a HIPAA requirement that is necessary for uniquely identifying patients and having an audit log. It was noted that instead of embedding intelligence into the ID, it is useful to have the only characteristic be that it is unique. It was also mentioned that this password cannot be secret to the HIE

P2 -- When an individual is granted access to patients' health information through an HIE from a particular organization participating in an HIE, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.

Discussion/analysis: **New** -- The word "should" was questioned but it was noted that these are recommendations not directives. The various HIEs have different options of responsibility so the word "should" allows HIEs to use the document as a guideline or checklist rather than as specified actions. Per our last discussion, organizations need to perform periodic reviews of HIE access to catch terminations or changes in position which would also change the individual's access controls.

Possible resources for future activities: **New** -- Other HIEs and the Markle Foundation's *Connecting for Health*.

Recommended stakeholder involvement: **New** -- Stakeholders include operations security, credentialing staff of health information managers along with IT, HR and legal. User agreements should describe the common process. Physicians and allied health professionals are required to be re-appointed on a bi-annual basis (periodic review required by JACHO).

P3 -- The ability of individuals to access patients' health information through an HIE should be set using role-based access standards which are developed and accepted by all organizations participating in an HIE.

Discussion/analysis: **New** -- It was mentioned that there will be different roles in the HIE. Different providers might have slightly different access standards. How does the HIE

reconcile these differences? Must HIE have common standards? It was pointed out that for the foreseeable future the HIE will only have access to part of an organization's EHR and each organization must have access controls for all of their employees' access to the complete EHR. This principle includes administrative and other non-medical staff that requires access to do their jobs.

Using a role-based context is a suggested requirement of HIPAA. Also Models of Care may be useful in this area.

Possible resources for future activities: **New** -- AHIMA and/or HIMSS may have some guidelines and Diane will check on what is available.

Recommended stakeholder involvement: **New** -- Stakeholders include operations security, credentialing staff of health information managers along with IT, HR and legal. User agreements should describe the common process. Physicians and allied health professionals are required to be re-appointed on a bi-annual basis (periodic review required by JACHO).

P4 -- All organizations participating in an HIE should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through an HIE. 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/analysis: **New** -- The security credentialing process needs to be streamlined from an ease of use perspective while still being thorough and adequately secure. A process that takes days instead of hours/minutes will inhibit provider acceptance. For example, the current CHIC authorization/authentication process can take one to two weeks.

Possible resources for future activities: **New** -- The experiences of other operating HIEs; such as, CHIC in Duluth.

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, HR, Medical Credentialing (JACHO does require a bi-annual reappointment of medical professionals) plus providers/users.

P5 -- Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in an HIE when

the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

Discussion/analysis: Medical credentialing was an authorization issue that was discussed at the group's first meeting. It was pointed out that the difference between access to paper records, for example faxing a record, and electronic access is that in the paper world, a practitioner gets access to a single record where electronic access, most times, means access to all an organization's records. It was argued that medical credentialing is different than security credentialing. Medical credentialing means verifying licensure and other institutional requirements, which helps, determines what privileges and role-based access they are granted. It was suggested that medical credentialing overlays technical or security credentialing and is not easily teased apart in some organizations. Terms of use agreements might be a partial answer to eliminate the confusion around the need for medical credentialing in the electronic exchange of healthcare data.

Possible resources for future activities: **New** -- JACHO and Medicare participation contracts. Also, IHE's Cross-Enterprise Document Sharing

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, HR, Medical Credentialing and Medical Affairs (JACHO does require a bi-annual reappointment of medical professionals) plus providers/users.

AUTHENTICATION

P6 -- All organizations participating in an HIE should minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.

Discussion/analysis: **New** -- In addition to a HIPAA requirement this principle is a corollary to P1 under Authorization. This issue should also be addressed by the HIE and each participant under the Assumption A5.

(Note Definition - **Single-factor Authentication** – This is when only one of the three possible factor types is used to authenticate a person for system access. The three factor types are:

1. Something you know, such as an ID and password or PIN.
2. Something you have, such as, a security fob or smart card (a physical object that must be presented to enable access).
3. Something you are, such as, personal biometric (fingerprint, retina scan, etc.), which is unique.)

This should be accomplished taking into consideration the different models of care and convenience factors.

Possible resources for future activities: **New** -- HIPAA requirement

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, and providers/users.

P7 --All organizations participating in an HIE should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the HIE (i.e., across participating organizations).

Discussion/analysis: **New** -- Access by individuals outside of a participant's organization should require an additional factor of authentication.

Possible resources for future activities: **New** -- National activities of the HHS AHIC's Confidentiality, Privacy and Security Workgroup, the eHealth Initiative's Technology Workgroup, other ARHQ funded activities in eAuthentication should be monitored. Also, how are other operating HIEs handling this issue today.

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, and providers/users.

P8 -- Authentication of individuals accessing patients' health information through an HIE should be as seamless as possible when accessing information across participating organizations.

Discussion/analysis: This principle is about making the process user-friendly or the process won't be used. Without this providers will be disinclined to access patient health information, thereby potentially reducing the quality of patient care. The 4A subgroup emphasized that it is always tempting to err on the side of security to the point where the system becomes unusable. The electronic exchange of data should be customer-friendly or it will not be used.

Possible resources for future activities: **New** -- Liberty Alliance (Use Cases), CHIC, IHE's Cross-Enterprise User Authentication, and other ARHQ funded eAuthentication projects. (An Identity Management PowerPoint from the University of Texas will be sent to the listserv complements of Christina Stephan.)

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, and providers/users.

P9 -- From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through an HIE should be the same process regardless of which participating organization's health information is being accessed.

Discussion/analysis: This principle emphasizes that the end-user needs to have the same process no matter which organization they are at, regardless of what underlying architecture the organization is using. It was mentioned that the patient consent group was concerned about how special protections afforded to mental health or substance abuse patient information were to be observed. By just knowing that a patient had health information at a facility like Hazelden, you know more about the patient than laws like

SAMHSA and other intended. It was suggested that to see sensitive information, the provider might need to re-authenticate. Another suggestion was that the role-based access is perhaps the better way to handle this question. Others agreed that the primary question is how you define sensitive information.

Possible resources for future activities: **New** -- HIMSS/GSA e-Authentication Pilot and EHR Vendors

Recommended stakeholder involvement: **New** -- IT Security and Operations, Business Health Information Managers, and providers/users.

ACCESS CONTROLS

P10 -- 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/analysis: This is an ideal principle. Studies show that a policy that is too restrictive can be detrimental to patient care. This principle focuses on the “need to know” principle and is implemented primarily through behavioral controls rather than just technological controls. Certain data sets (mental health, chemical dependency, HIV/AIDS, etc) have more stringent protections placed around them.

There are two types of major controls, behavioral controls and hard controls. Behavioral controls consist of things like policies and education, hard controls consists of things like the “break the glass” function and segregation of data sets. Behavioral-dependent controls require policies, education and sanctions if the policies are violated.

This principle may prove extremely difficult to implement because all information may prove relevant to treatment. Currently the maturity of the technology and its users’ ability to successfully use this technology do not allow organizations the ability to adequately restrict access.

New Discussion -- (Note Definition - **Treatment Relationship** - 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. SOURCE: HIPAA)

Possible resources for future activities: **New** – NA

Recommended stakeholder involvement: **New** -- This is basically a training issue; therefore, HR, CPO, Corporate Compliance, Integrity Training etc. should be involved.

P11 -- All organizations participating in an HIE should develop and accept written policies and procedures for accessing and exchanging patients' health information through the HIE.

Discussion/analysis: We need a policy and technical approach that allows access control to keep information flowing among people authorized to see it and protected from unauthorized access or use. The selection and implementation of policy and technical elements are themselves aids or obstacles to privacy and security.

Possible resources for future activities: **New** -- Markle Foundation's 'Connect for Health' and eHealth Initiative.

Recommended stakeholder involvement: **New** -- Legal, HR, CPO, Corporate Compliance, etc. should be involved.

5. Wrap-up/Next Meeting

Mike Thorsen reminded the group next meeting of the AAAA Subgroup will be Wednesday, January 10, 2 – 4 pm, at the HealthPartners Conference Center in the Pine Room. Mike also recommended that group members send new or edited principles or definitions as well as white papers or articles that they think might be helpful to the group.