



Consent Aggregation

Beyond Basic “Opt-in” or “Opt-out”

(Managing consents in one, or across multiple applications)

February 2007

Version 3.4



“Any health network needs privacy protection built in. Privacy must be an essential component. The fundamental right of privacy should determine the architecture of the system. Technology should serve our values, and be determined by them – not the other way around.”¹

“Without strong safeguards, reliable privacy protection, and vigilant enforcement of privacy laws, public support for the national effort to develop a healthcare network could be in jeopardy.”²

“While patients are eager to have better access to their own records, to have their providers more aware of their health data, and to see systems streamlined, co-ordinated and integrated – they do have serious concerns about privacy, security, accuracy and the user-friendliness of the systems themselves.”³

Introduction

Government legislation, organizational policies/practices and patient requests all govern how protected/personal health information (PHI) must be managed and disclosed. A major concern for Care Delivery Organizations (CDO) today is the ability to protect PHI in a single application – while satisfying the aforementioned – or to do this across multiple applications on a networked workstation or web-portal.

Many working in healthcare information technology (HIT) today believe that it is sufficient to allow a patient to simply “opt-out” of having their records available in electronic form – should the patient express concerns about the privacy of their PHI. However, it is widely recognized that there are greater societal benefits (e.g. biosurveillance) to have as many patients as possible agree to “opt-in” – and stay in.

Therefore, a method which allows a patient to restrict access to a particular record (e.g. lab report), or document arising from a particular encounter, while allowing access to the remainder of the electronic medical record is beneficial to all. The question then becomes:

How does a CDO manage consents at a granular level across multiple applications?

Consent Aggregation

Consent Aggregation is the term used to define the process of managing multiple stakeholder consent directives⁴, at a granular level, across one or more applications. For a CDO to effectively achieve Consent Aggregation it is required to follow three basic elements.

1. Patient-imposed consent directives and CDO policies must be defined and automated for use in governing access to a patient’s PHI.
2. Distribution and application of these directives and policies must be made to the application(s) where access to PHI occurs.
3. Compliance with these directives and policies must be monitored through comprehensive auditing.



Elements

1. Patient-imposed consent directives and CDO policies must be defined and automated for use in governing access to a patient's PHI

Patient-imposed consent directives and CDO policies must be used to govern access to a patient's PHI

Defining patient-imposed consent directives

In the many jurisdictions where privacy legislation now exists, a patient has the right to place a restriction or allow access regarding the use and disclosure of their PHI in the form of a consent directive. These patient-imposed directives take precedence over the privacy policies specified by the CDO.

Defining a CDO privacy policy

A CDO privacy policy can vary from the general (healthcare information may be accessed for the benefit of the patient), to the specific (healthcare information, "X", can only be accessed by physicians "A", "B" or "C" if situation "Y" arises). The various elements included in a privacy policy may be quite numerous. These elements may include, but are not limited to the:

- user/caregiver accessing the information (name, role, group, location, etc.)
- patient (name, classification, location, etc.)
- information being accessed (sensitivity, scope, reason, etc.)

A good example of a CDO policy is one that outlines special access restrictions to PHI for patients who are also staff members. This policy would be easily implemented by a set of system level directives that apply to this group of patients. Hence, tagging a patient as a staff member would render their PHI inaccessible by other staff members.

The evolution of directives

In paper-based practices, a patient may request that access be restricted to a document containing their PHI. In this case the healthcare provider seals the document in an envelope and records the restriction in the patient's file.

The electronic equivalent is to record the restriction in the on-line copy of the document, and possibly even encrypt the on-line copy for security. However, this is not entirely satisfactory because:

- the patient may not know which PHI document to restrict
- there may be multiple documents affected by the directive
- multiple documents/copies may already be distributed into the record system



- there may be past or future documents affected by the directive

Automating directives

The key to automation is to create access rules, herein referred to as “consent” directives when applied to patient level information or “system” directives when applied at a system level.

It is necessary when automating the process to provide separation between the directives and the affected PHI. It is easy enough to associate PHI with directives via a common denominator (e.g. patient identifier) and while it certainly is possible to restrict a particular document by explicitly naming it in the consent directive, there is additional criteria that can be used to associate directives with groups of PHI. An example of this is the clinical encounter identifier which identifies all PHI created or updated during a particular visit to a caregiver.

2. Distribution and application of these directives and policies must be made to the application(s) where access to PHI occurs

To make Consent Aggregation work, client applications attempting to access PHI must first access the system and consent directive information – which are PHI themselves – to determine whether access is permitted.

Therefore, there is a need in Consent Aggregation for every clinical application to apply the system and consent directives when retrieving, displaying and modifying PHI. However, in reality this is likely to be impractical. The number of legacy applications in use and the fact that there are a number of different applications on a single workstation operating with similar clinical data, results in a redundancy of operations.

It is more efficient to have a mechanism that abstracts the consent management component from the clinical applications and services all the applications on a particular clinical workstation.

3. Compliance with these directives and policies must be monitored through comprehensive auditing

“The existence of an audit trail ensures that charges of privacy incidents can be investigated based on documented records and not rely solely on the word of one employee against another. Audit systems can also deter employees from inappropriately accessing information, because employees are aware their data access is being monitored.”⁵

Consent Aggregation is not complete until comprehensive auditing is in place.



HIPAAT's Solution

HIPAAT's approach to Consent Aggregation has three main components which, when used in conjunction with CCOW, provides a powerful yet relatively simple approach to Consent Aggregation.

The three components are:

1. Privacy eSuite™
2. Privacy Manager™
3. Universal Audit Repository™

HIPAAT has adopted a client-server model allowing the management of consent and system directives to be server-based, the evaluation of the directives to be either server or client based and the application of the directives to be performed on the client side. The client application provides directives information to the user/caregiver as well as collecting information used in privacy auditing.

Privacy eSuite

As a web-based privacy document management system it manages patient lock box/consent directives, requests to access/correct PHI, disclosures and privacy-related complaints. This server solution works with the assumptions that:

- application of a directive is best carried out by the client application that interfaces with the user/caregiver
- the directives need to be accessible to all client applications and a server network is most appropriate for this

There are many directives to consider. Hence, it is better to utilize a single privacy server to perform this function – thus eliminating the need for checking in every client application.

Privacy Manager

A software product that integrates with hospital architecture (e.g. HL7 CCOW) to allow healthcare providers to manage user access to patient PHI based on directives established by the patient, substitute decision-maker or the CDO. Access to PHI generates an Integrating the Healthcare Enterprise (IHE)-compliant audit trail.

The Privacy Manager provides an on-screen notification to the caregiver about the privacy status of the PHI for each patient in question. Warnings or alerts are displayed where required and caregivers have the ability to override directives, or deny access where appropriate. It is advantageous to consider the Privacy Manager as a loosely-coupled, vendor-independent feature of a clinical workstation or portal, rather than an integral feature of a clinical application.

Universal Audit Repository (UAR)

The UAR is a stand-alone central repository of privacy/security events. It provides simple yet extensive search and report

As of February 2007:

HIPAAT's Consent Aggregation solution also works via simple application interface (API). HL7 CCOW, though effective, is not required.

For more details, check back soon at www.hipaata.com.

HIPAAT understands the requirements and provides a solution to simplify management of consents at a granular level across multiple applications – also known as Consent Aggregation.



capabilities. Also, it generates and manages administrative follow-ups. (Including PHI accessed email alerts.) This product accepts ATNA XML audit messages - including HL7 CCOW context changes, from any source that follows the IHE-defined audit log schema.

HL7 Clinical Context Object Workgroup (CCOW)

CCOW was developed for synchronizing data between clinical applications. This process is also known as “Visual Integration” or “Patient Synchronization.” As it relates to the Privacy Manager, CCOW operates on a clinical workstation or portal environment as follows:

1. All applications operating on a workstation register with the CCOW Context Manager.
2. Before an application accesses and retrieves PHI it applies to set the clinical context with the Context Manager indicating the information being retrieved. Typically this information includes the identifier of the user (set after authentication), the identifier of the patient and some information on the PHI being accessed, such as an order number, encounter number, creation date, etc.
3. All other applications are notified of the pending context update, including the Privacy Manager.
4. Typically the other applications accept the new context change, and the initial application proceeds to access and display the PHI to the user.
5. However, if the Privacy Manager application detects a potential access violation or an issue relating to the new context, it will:
 - a) with override – put up a message that informs the user that such an operation may be unauthorized or improper
 - b) deny access – reject the context change and cause the initial application to abandon the operation
6. Logging of the context changes provides the necessary audit trail to keep track of access to PHI.
7. Generate a privacy/security alert.

Using CCOW in combination with the Privacy Manager has the following advantages:

- CCOW is an existing standard that is growing in acceptance as more vendors, including the leaders in the healthcare industry, adopt it
- many of the requirements of CCOW, such as authenticated-user identification and a well-defined set of subject elements are necessary for Consent Aggregation
- CCOW-compliant clinical applications do not have to change much, if at all, to support the Privacy Manager. Therefore it



can – to a large extent – be implemented seamlessly into existing installations

Non-CCOW-compliant applications can be made compliant via a number of different techniques; there are companies already performing this task.

Conclusion

Effective consent management facilitates the needs of all stakeholders as it relates to the privacy and security of healthcare information when managing consents in one, or across multiple applications.

The patient is empowered by the CDO to participate in how their electronic PHI is to be viewed. Further, a CDO can benefit from having the greatest number of participants in their EMR system.

This client-server model of managing consents can be introduced in a proprietary environment, but is most effective when deployed in an environment where HL7 CCOW context management is present. Moreover, the existence of an audit trail ensures that privacy/security alerts, or accusations of privacy incidents, can be easily investigated.

Consent Aggregation, when properly implemented, provides the framework that allows the consumer to go beyond an all-or-nothing choice – to go beyond “opt-in” or “opt-out.”

Note: HIPAAAT's approach makes it appropriate for use as part of a national EHR⁶, NHIN⁷ or RHIO/LHIN⁸.

-
1. Radwanski, George. [Privacy Commissioner of Canada] Patient Privacy in the Information Age. E-Health 2001: The Future of Health Care in Canada. Toronto, Ontario. 29 May 2001.
 2. Bishop, L.S., et al. “National Consumer Health Privacy Survey,” California HealthCare Foundation. November 2005.
 3. Weinberg, Myrl, CAE. Closing Session. HIMSS Summit: Achieving National Healthcare Transformation. The Renaissance Hotel, Washington, D.C. 07 June 2006.
 4. Consent directives: rules governing access to PHI
 5. Markle Foundation. “The Privacy and Security Working Group.” Report and Findings. June 2003
 6. EHR – Electronic Health Record
 7. NHIN – Nationwide Health Information Network
 8. RHIO/LHIN – Regional Health Information Organization / Local Health Integration Networks