Creating an IHE ATNA-Based Audit Repository

Bill Gregg, Horacio D'Agostino, and Eduardo Gonzalez Toledo

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) requires gathering audit information from picture archiving and communications systems (PACS) regarding evidence trails of human interactions. Until recently, most PACS users have had limited access to auditing information. Access required resources to handle manual inspection of audit logs, and access to proprietary databases was not always available. Some vendors now produce eXtensible Markup Language (XML) audit logs based on certain events occurring in PACS. However, it is up to the user to convert this information into an easily mined data repository supporting compliance and quality control. This process can be handled in multiple ways, which could mean different audit mechanisms depending on the PACS (or other hospital system) used. It is apparent that an organized method of dealing with audit information is needed. This help may be provided within the Integrating the Healthcare Environment (IHE) framework. The IHE initiative defines a set of profiles, actors, and transactions that create common scenarios for particular workflow processes. The Integration Profiles depict security as a fundamental requirement of the framework. Specifically, the Audit Trail and Node Authentication (ATNA) profile defines standards based mechanisms for securely transmitting and storing audit records in a central repository. The data structure defined by the profile provides a number of record types that capture different audit events. A general feasibility study for storing currently available PACS audit information following the profile is defined, and steps to an automated solution are discussed.

KEY WORDS: Audit, audit trail, IHE, ATNA, NET, XML, Microsoft Access

BACKGROUND

Prior to this project, there was no well-defined mechanism to evaluate user interaction within the current PACS. Audit records containing user interaction information were stored in multiple

locations. It was theoretically possible to mine these logs, but it required training and log documentation. This was a tedious manual process that was generally not performed due to lack of knowledge and time. Efforts to deal with this complexity in a structured manner have been documented¹⁻³. A more centralized picture archiving and communications systems (PACS) audit capability was introduced, creating a simple eXtensible Markup Language (XML) data file of events. The data file could be obtained by the institution to manipulate as they saw fit. This provided a significant step and the impetus to create a mechanism outside of PACS to use that data.

Accountability of human interactions with PACS is necessary to improve the PACS process and provide quality control. Without this information, errors continue to occur. On April 14, 2003, Health Insurance Portability and Accountability Act (HIPAA) set rules regarding privacy for Protected Healthcare Information (PHI)⁴. These rules are found in the U.S. Code of Federal Regulations (CFR), Title 45—Public Welfare, Part 160—General Administrative Requirements, and Part 164—Security and Privacy. To comply with these requirements, hospitals should limit human interactions with patient data to what is “minimal and necessary”. This is a difficult task,

From the Department of Radiology, LSU Health Sciences Center, Shreveport, LA, USA.

Correspondence to: Bill Gregg, Department of Radiology, LSU Health Services Center, Shreveport, LA, USA; tel: +1-318-6756237; fax: +1-318-6756351; e-mail: bgregg@lsuhsc.edu

Copyright © 2006 by SCAR (Society for Computer Applications in Radiology)

Online publication 18 September 2006

doi: 10.1007/s10278-006-0927-7

particularly in a teaching institution where access limitations hinder learning and patient care and are administratively complex. In a more “reasonable and appropriate” access atmosphere, there still must be a way to monitor these interactions. A viable mechanism to deal with this is to utilize audit logs to perform periodic review of human interactions⁵. In conjunction with policies and procedures regarding inappropriate access described in 45 CFR Section 160.308(a) 3–6, audit information can support administrative action.

Hospitals are now faced with two dilemmas: how to audit systems, and how to manage the audit information in a consistent and economical manner. It is not practical to try to manage each system’s audit information separately. HIPAA regulations described in 45 CFR Section 164.530 also promote a single source for audit reviews, and this has translated into the position of Security Officer in most hospitals. The “gold standard” in

this case is to push audit records from all systems into a central repository that can be mined by the Security Officer.

Efforts to help hospitals are evolving within Integrating the Healthcare Environment (IHE), now formally in its seventh year⁶. Its purpose is to provide a common framework of profiles, actors and transactions that describe common working scenarios in systems and their interfaces. This common framework is based on standards such as digital imaging and communication in medicine (DICOM) and HL7. This is intended to ensure the same outcome regardless of what vendor is providing the actors that get the work done.

The profile chart described by IHE (Fig. 1) puts the ITI Audit Trail and Node Authentication (ATNA) profile at the foundation of all the other profiles. It defines a secure method for sending and receiving audit information, and a common

Fig 1. IHE integration profiles.

Fig 2. ATNA schema to access database.

data structure to be used. Within a profile, the process of an actor performing transactions could cause trigger events to occur which require the creation of an audit record. The IHE working groups provide a generic mechanism for consolidating audit logs by describing an audit data schema in the IHE IT Infrastructure Technical Framework^{7,8}. This contains several profiles designed to provide a consistent mechanism for dealing with the many auditable events that routinely occur. The DICOM Audit Message Vocabulary^{9,10} extends the basic vocabulary defined in the schema. The Provisional IHE Audit Message format described in the now deprecated Basic Security Profile is used to define the database tables in this project.

We report in this article a method created to provide a primary layer of compliance with HIPAA, and to begin utilization of the IHE ATNA profile. The key focus for this process is to help understand the ATNA profile and how it might support automated auditing.

METHODS

The materials utilized on this project involve software, hardware and the hospital network. The program development, database, and the program software used are:

Microsoft Visual Studio .Net 2003/2005 (specifically Visual Basic .Net and the .Net framework 1.1,2.0)
PACS Auditor program (created in Visual Studio .Net)
Microsoft Office 2003 Access

Fig 3. PatientRecords table.

Fig 4. ProcedureRecords table.

PACS_Audit database (created in Microsoft Office 2003 Access)

The project runs on a Dell Dimensions 8300 computer with a 3.0-GHz Intel Pentium processor with 1 GB of RAM and a 120-GB Raid 1 (mirrored) hard drive array.

The General Electric (GE) PACS Version is Centricity 2.0 CSR5 SP2

The hospital network consists of a Gigabit fiber backbone with 10/100 switched connections to the desktop. The institutional perimeter has security implemented by the

Fig 5. UserAuthenticated table.

network group. It provides the conduit for moving daily XML audit log files generated on the PACS to the Dell computer where it is manipulated and stored in the database. Routine backups are done, and the media is stored off-site.

This project includes a single table for storing the XML output, and other tables designed to emulate the Provisional IHE Audit Message format. These ATNA tables will initially be limited to the ProcedureRecord, PatientRecord and User-Authenticated records. Currently, only these record types are transmitted in the XML file. A main Audits table was created as the master index for all records pointing to the appropriate subordinate data table. Figure 2 depicts the pertinent IHE Year 4 schema elements on the left, and the corresponding Access database tables on the right.

The default ATNA schema does not include data elements for all the parameters provided by the PACS. Extensions have been added to the data tables to accommodate this useful data and are designated by the prefix "X_" (Figs. 2, 3, 4, 5). The data involved includes Exam Changes (canceled, arrived, verified, dictated, completed, and reference only), Exam Merges, Patient Merges, Exams Viewed and Printed, and User Logins/Logouts. The schema to Access table correspondence is graphically displayed below with the ATNA schema on the left and the Access table on the right. Connecting lines are used to

identify corresponding data fields. Figure 3 shows the Patient-Records table, Figure 4 shows the ProcedureRecords table, and Figure 5 shows the UserAuthenticated table.

The XML file is created daily on the PACS, and exported to the Dell computer. The PACS Administrator collects and analyzes the data.

The following procedure is utilized for this study.

1. Gather audit information from the PACS.
2. Move the XML log files to the computer used for storage of the audit information.
3. Execute the PACS Auditor program to verify and import the data into Access.
4. Utilize forms and reports to query the data as needed.

RESULTS

The XML files are retrieved from the PACS and the PACS Auditor program is used to read them. Once a file is loaded into the internal data

Fig 6. The PACS audit log loader program.

structure, the fields can be bound to the form to display the records (Fig. 6). This data can be viewed but not edited directly. Although there are few reasons to review this data here, the application can help pinpoint data errors that may occur in the XML file.

A completed data set created from the XML file is pushed to the database by clicking the Upload button. A form in the database allows for multiple criteria selection, and the ability to create different forms and reports based on these criteria (Fig. 7).

Login monitoring referred to in 45 CFR Section 164.308(a)(5) can be done by clicking the "Logins/Logouts" button. Although login failures are currently not recorded, the occurrence of

overlap logins that may indicate multiple users logging in with the same ID can be performed. Section 164.312(b) requires audit controls to record and examine PHI activity, and Section 164.312(c) addresses integrity of data and the protection of PHI from alteration or destruction. Also, Section 164.528 allows an individual the right to receive an accounting of certain disclosures of their respective PHI made by a covered entity.

To satisfy these requirements, the following questions should be easily answered by the database.

1. All activity for a particular patients account.
2. All activity for a particular user.

Audit_Form : Form

PACS Audit

Auditing Selector

Start Date Stop Date
 Start edt Stop edt

Accession Number
 MR Number
 User ID
 Event Type
 Exam Status
 Workstation

☐ All Fields ☐ Summary

Exit the Application

Fig 7. Database reporting screen.

3. All or specific activity within a time frame.
4. Specific actions performed on an exam that change related information.

These questions can be easily answered to the extent of the original data provided by using the available selection criteria fields, and then selecting one of the available form or report buttons. Any desired date range can be selected, and a search by medical record number or user ID can be done to answer questions 1 and 2. This will show all PHI activity in PACS as described in Methods. This can be viewed as an Access data sheet form for easy manipulation, or as a report preview, which can be printed if necessary.

Other specific actions such as exam and patient merges done, other event types, and specific work station usage can be audited by filling in the appropriate selection criteria. One such action would be to keep track of emergency login ID

use. All emergency login IDs in the PACS start with "EM", which can easily be specified in the User ID pattern match criteria field. The Audit Data Sheet provides the most relevant fields for quick review (Fig. 8). Events such as exam and patient merges, films printed, and specific status changes are highlighted in color in the form for easy visualization. The "All Fields" check box allows all field information sent from PACS to be viewed. This additional information is often helpful in determining what exam was merged as that exam no longer resides in the database.

Quality control and continuing education are also supported by the mechanisms listed above. It becomes relatively easy to determine who is merging exams or patients, or verifying or dictating exams. This can be incorporated into an ongoing Quality Control process to evaluate issues that arise, and to promote ongoing education. The Exams Printed report can be used to monitor

Audit_Log_Form										
	Date	MR Num	Name	Acc Num	Event	Status	User	Wks	Study Date	Procedure
	3/30/2006 7:42:26 AM	947	Patient948	1807	EV	50	User51	CEN036	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 7:43:00 AM	947	Patient948	1807	EV	50	User51	CEN036	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 7:43:58 AM	947	Patient948	1813	EV	60	User51	CEN036	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 7:47:37 AM	947	Patient948	1807	EV	50	User51	CEN036	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 8:02:33 AM	947	Patient948	1813	EV	60	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:09:12 AM	947	Patient948	1813	EV	60	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:09:59 AM	947	Patient948	1813	EC	40	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:10:07 AM	947	Patient948	1813	EV	40	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:12:54 AM	947	Patient948	1813	EC	10	RIF	BROKER	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:13:28 AM	947	Patient948	1813	EV	10	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:15:05 AM	947	Patient948	1807	EV	50	User27	CEN050	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 8:15:25 AM	947	Patient948	1813	EV	10	User27	CEN050	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:16:24 AM	947	Patient948	1807	EV	50	User27	CEN050	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 8:16:58 AM	947	Patient948	1864	EV	10	User27	CEN050	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:19:06 AM	947	Patient948	1864	EM		User27	LSU003		
	3/30/2006 8:19:16 AM	947	Patient948	1813	EC	10	User27	LSU003	20060329133357	L FOREARM 2 VIEWS
	3/30/2006 8:23:00 AM	947	Patient948	1864	EC	40	User27	LSU003	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:23:17 AM	947	Patient948	1864	EV	40	User27	CEN050	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:24:14 AM	947	Patient948	1864	EC	50	User27	CEN050	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:26:06 AM	947	Patient948	1864	EV	50	User51	CEN036	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:47:02 AM	947	Patient948	1864	EV	50	User27	CEN050	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 8:54:05 AM	947	Patient948	1864	EV	50	User143	CEN054	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 9:34:46 AM	947	Patient948	1864	EC	60	User51	CEN036	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 9:45:45 AM	947	Patient948		PM		User27	LSU003		
	3/30/2006 9:46:13 AM	947	Patient948		PM		User27	LSU003		
	3/30/2006 9:48:01 AM	947	Patient948	1807	EC	40	User27	LSU003	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 9:49:04 AM	947	Patient948	1807	EM		User27	LSU003		
	3/30/2006 9:50:07 AM	947	Patient948	1807	EM		User27	LSU003		
	3/30/2006 9:51:00 AM	947	Patient948		PM		User27	LSU003		
	3/30/2006 9:51:20 AM	947	Patient948	1807	EM		User27	LSU003		
	3/30/2006 9:52:05 AM	947	Patient948	1807	EV	40	User27	CEN050	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 9:53:09 AM	947	Patient948	1864	EV	60	User27	CEN050	20060329133357	R FOREARM 2 VIEWS
	3/30/2006 9:53:26 AM	947	Patient948	1807	EV	40	User27	CEN050	20060329170223	R FOREARM 2 VIEWS
	3/30/2006 9:54:52 AM	947	Patient948	1864	EV	60	User27	CEN050	20060329133357	R FOREARM 2 VIEWS

Fig 8. Audit data sheet form.

printing activity and help address HIPAA and institutional policy issues. This report allows summarized counts per user, or detail per user of the exams the print was performed on.

The data loaded into the ATNA tables described above provides the first steps in the evolution of this process. The original single table data is still available while progress toward the ATNA structure is developed. As this structure becomes more standardized, reports can be created from this data, and the single original table can be dropped.

DISCUSSION

Utilization of XML is becoming ubiquitous, and there are many possible mechanisms for accessing data the files hold. The imported data is to be converted to the appropriate fields in the IHE ATNA schema structure. This method uses three of the many event records described in the provisional schema. The ATNA Profile recommends using only data defined in its schema. However, as described in Figures 2, 3, 4, 5, there are significant schema extensions required to accommodate all useful audit information. Strict event auditing may only require this defined structure, and additional information may be vendor-specific, but it is often necessary to correctly interpret changes in the data.

The primary Audits table uses a "Host" field to designate where the audit record originated. This could be from the PACS, the laboratory system, or any other health care system that stores PHI. Health care environments today often comprise more than one facility as separate institutions are merged, or organizations connect to Regional Healthcare Information Organizations (RHIO). The subsequent decision on where audit repositories will be kept must be made, and the need to audit data both at the enterprise and the facility level exists. Although one could include facility codes in the "Host" field to facilitate these types of searches, it would be best to incorporate a separate "Site" field as well.

The current project is a start toward the ultimate goal of providing an IHE ATNA-based central audit repository. It is critically important to provide a central time server in the proposed state of multiple devices sending IHE audit information.

In this case, only the PACS is sending information and consequently fulfills the role of time server. As other systems begin to participate, a central time server will be necessary. There are several known issues in the current implementation:

1. There is an incomplete set of event information.
2. There is no secure transport mechanism between the audit event creator (PACS) and the receiver (the described PACS Auditor program).
3. There are no audit events created as a result of administrative review and manipulation.
4. Stricter security should be implemented, which will be facilitated by a move to a fully relation database.

The ATNA profile data should correspond to transactions that are performed by IHE actors. To properly capture and manipulate this data, it must be stored in a meaningful way. A common set of audit record trigger events is defined in the IHE structure. This event data should be incorporated into the audit record, and then sent to the central repository. Currently, very few IHE profiles, actors, and transactions are actually provided by vendors. It is anticipated that consumer feedback will improve this situation over time.

This leaves several other issues to be considered:

1. The ATNA XML audit record can be used in several scenarios providing varying levels of automation. Customizations are needed if the process is not fully automated.
2. These scenarios need to be examined to determine if full automation can be achieved. The following questions need to be asked:
 - a. Can the ATNA schema define audit data such that extensions are not needed?
 - b. Will vendors create audit records that fit this schema?
 - c. Can software systems automatically load data from this audit record into a repository without customization?
 - d. Once the data is in the repository, can the database tools available allow easy data mining?
 - e. How feasible will it be for institutions to work with systems that can not be fully automated?
3. All institutions should gain a greater understanding of IHE in general. This is by necessity

a large undertaking, but the benefits gained from standardized systems are evident both within and outside of health care.

A long-term goal may be to securely store all appropriate audit information in a central repository while giving the institution the ability to fully mine the data. This would eliminate the need to store redundant audit data elsewhere to support Quality Control programs. Moving from the provisional audit format to the currently recommended format may provide this ability, and is the next step in this process.

CONCLUSIONS

The methods described in this study provide a foundation for compatibility with the IHE ATNA profile. The reporting capabilities offer baseline methods for providing compliance with HIPAA regulations and institutional policy. Although much remains to be done, the feasibility of this approach is promising. It is clear that keeping up with DICOM and IHE additions and changes is a complex process. A successful incorporation of these developing standards and frameworks requires a team effort between institutions and vendors. An educational process to bridge the gap between the standards bodies and the implementers is recommended. Achieving the end result of these efforts will simplify complex implementations, and a fully automated central solution should be the goal.

Every medical entity should have the ability to access and store audit information regarding the trigger events described in the IHE ATNA Profile. The vendors are encouraged to work on providing ATNA-based audit records. Users should continue

to develop tools to organize and provide this information to support institutional policies and legal requirements. Support for the efforts outlined in the IHE framework is critical to ensure easy and consistent integration of relevant data throughout the enterprise. This will result in a win-win situation for both the user and the vendor.

REFERENCES

1. Liu BJ, Zhou Z, Huang HK: A HIPAA-compliant architecture for securing clinical images. *J Digit Imaging* 19 (2):172–180, 2006
2. Huang HK: *PACS and Imaging Informatics (Basic Principles and Applications)*. New Jersey: Wiley-Liss, 2004
3. Coleman RM, Ralston MD, Szafran A, Beaulieu DM: Multidimensional analysis: a management tool for monitoring HIPAA compliance and departmental performance. *J Digit Imaging* 17 (3):196–204, 2004
4. HIPAA, <http://www.cms.hhs.gov/HIPAAGenInfo/>, 45 CFR Parts 160, 162 and 164, Health Insurance Reform: Security Standards; Final Rule, 02/20/2003
5. IHE IT Infrastructure Technical Framework, Volume 1, Rev 2.0, 08/15/2005, p. 57, 9.2.1 Audit Messages
6. IHE, <http://www.ihe.net/TechnicalFramework>, IHE Technical Framework Volumes 1–6, Integration Profiles, Rev 6.0, 05/20/2005
7. IHE IT Infrastructure Technical Framework, Volumes 1–2, Rev 2.0, 08/15/2005
8. Marshall G: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, The Internet Society, Network Working Group, RFC 3881, 2004
9. IHE IT Infrastructure Technical Framework, Supplement 2004–2005, Audit Trail and Node Authentication Profile (ATNA), Trial Implementation, 08/15/2004, 3.20.7 Audit Message Formats
10. Digital Imaging and Communications in Medicine (DICOM), Supplement 95: Audit Trail Messages, Trial Use Draft, 06/18/2004