HIPAA and WorldVistA

Presentation To WorldVistA Community Meeting
January, 2008

George Lilly
David Whitten

Agenda

- What is HIPAA?
- Who must comply?
- HIPAA Security Rule Criteria Certified By CCHIT
- HIPAA Claims Attachment Rule And The CCD

What is HIPAA?

- **H**ealth **I**nsurance **P**ortability and Accountability **A**ct of 1996
  - Portability of health insurance coverage; subtitle with HIPAA rules
- Administrative Simplification Subtitle (ASS)
  - Privacy
  - EDI Transactions
  - **Security**
  - National Provider Number
  - **Claims Attachment**

Who must comply?

- The HIPAA law only applies directly to “Covered Entities”
  - Healthcare Providers
  - Healthcare Payers
  - Clearinghouses
- Software Vendors And Service Providers (for example, WorldVistA) Are Treated By HIPAA As “Business Associates”
  - Have a “Business Associates Contract” with a Covered Entity
  - Must meet obligations in the contract
  - Cannot on their own be “HIPAA Compliant”

There are 17 areas that must be implemented by every Covered Entity with written policies to comply with the HIPAA Security Rule

- **Administrative Safeguards**
  - **Security management process**
  - **Assigned security responsibility**
  - **Workforce Security**
  - **Access-Management**
  - **Training**
  - **Security incident procedures**
  - **Contingency plan**
  - **Evaluation**
  - **Business associate contracts**
- **Physical Safeguards**
  - **Facility Accesss Controls**
  - **Workstation Security**
  - **Device and media controls**
- **Technical safeguards**
  - **Access Control**
  - **Audit Controls**
  - **Integrity**
  - **Person or entity authentication**
  - **Transmission Security**

CCHIT Specifies Which Of Its Compliance Criteria Are Directly Relevant To HIPAA Security Provisions

	WG	Category and Description	Specific Criteria	Source or References * See end of document for references.
S1	Sec	Security: Access Control	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.	ISO 17799: 9.1.1.2.b; HIPAA: 164.312(a)(1)
S2			The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.	Canadian: Alberta 4.1.3 (EMR); CC SFR: FMT_MSA; SP800-53: AC-5 LEAST PRIVILEGE; HIPAA: 164.312(a)(1)
S3			The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)	Canadian: Ontario 5.3.12.e (System Access Management); CC SFR: FDP_ACC, FMT_MSA; ASTM: E1985-98; SP800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL; HIPAA: 164.312(a)(1)

WorldVistA Has Obtained CCHIT Certification And In The Process Has Been Verified To Have Specific Features Required By HIPAA

Sec	Security: Audit	Removed	
		The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)
		The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	CC SFR: FAU_GEN; SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION; HIPAA: 164.312(b)
		The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).	CC SFR: FAU_SAR; SP800-53: AU-7 AUDIT REDUCTION AND REPORT GENERATION; HIPAA: 164.312(b)

The CCHIT security features, if used properly, will enable a Provider to comply with the HIPAA Security Rule

Sec	Security: Authentication	The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.	Canadian: Alberta 1.1; CC SFR: FIA_UAU, FIA_UID; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION; HIPAA: 164.312(d)
		When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	Canadian: Alberta 7.3.12 (Security) Canadian Ontario 5.3.12.b (System Access Management); CC SFR: FIA_SOS, FIA_UAU, FIA_UID; ASTM: E1987-98; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION (no strength of password); ISO 17799: 9.3.1.d; HIPAA: 164.
		The system upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.	Canadian: Alberta 7.3.14 (Security) Canadian Ontario 5.6.12.a (Workstation Security); CC SFR: FTA_SSL, FMT_SAE; SP800-53: AC-11 SESSION LOCK; HIPAA: 164.312(a)(1)
		The system shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).	Canadian: Ontario 5.3.12.c (System Access Management); CC SFR: FIA_AFL, FMT_SAE; SP800-53: AC-6 UNSUCCESSFUL LOGIN ATTEMPTS, AC-11 SESSION LOCK ; ISO 17799: 9.3.1.e, 9.5.2.e; HIPAA: 164.312(a)(1)
		When passwords are used, the system shall provide an administrative function that resets passwords.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)

		When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.	CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)
		The system shall provide only limited feedback information to the user during the authentication.	CC SFR: FIA_UAU; SP800-53: IA-6 AUTHENTICATOR FEEDBACK; HIPAA: 164.312(d)

Sec	Security: Technical Services	The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.	Canadian: Alberta 7.4.6.2 & 8.4.6.2 (Technical); CC SFR: FCS_COP; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS; HIPAA: 164.312(e)(1)

WG	Category and Description	Specific Criteria	Source or References * See end of document for references.
		When passwords are used, the system shall not transport passwords in plain text.	Canadian: Ontario 5.3.12.a (System Access Management); CC SFR: FCS_CKM; SP800-53: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT; HIPAA: 164.312(e)(1)
		When passwords are used, the system shall not display passwords while being entered.	CC SFR: FPT_ITC; ISO 17799 9.2.3; HIPAA 164.312(a)(1)

Sec	Reliability: Backup / Recovery	The system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.	Canadian: Alberta 7.3.16 (Security); CC SFR: FDP_ROL, FPT_RCV; HIPAA: 164.310(d)(1)
		The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.	Canadian: Alberta 7.3.18.9 (Security); CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.310(d)(1)
		If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.	Canadian: Alberta 7.4.2.5 (Technica+D1I); CC SFR: FDP_ROL; HIPAA: 164.310(d)(1)

The system shall include documentation that itemizes the services (e.g. PHP, web services) and network protocols/ports (e.g. HL-7, HTTP, FTP) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).	CC SFR: AGD_ADM; SP 800-53 AC-5 CM-6; SP 800-70; HIPAA 164.312(a)(1)

The HIPAA Claims Attachment Rule Was Planned In 2005 To Be Based on the HL7 CDA

from the Federal Register 2005 where the Claims Attachment Rule was first proposed:

"In part 162, we would specify the ASC X12N Implementation Guide 004050X151 (ASC X12N 275—Additional Information to Support a Health Care Claim or Encounter and the **HL7 CDA**R1AIS0000RO21 HL7—Additional Information Specification Implementation Guide, and HL7—Clinical Document Architecture Framework Release 1.0) as the standards for conveying electronic health care claim attachments, and we would specify the following six specifications as the standards for the electronic health care claims attachments:"

However, since 2005, there has been no Notice of Proposed Rule Making (NPRM) issued for Claims Attachment.

- Many clinicians (notably ASTM) found that the CDA was not specific enough and machine-processable enough for clinical use and so since 2005 they have worked on enhancing the CCR instead
- The split between supporters of the CDA and supporters of the CCR held up the design of the Claims Attachment Rule until 2007
- In March 2007 HL7 and ASTM announced that the CDA and CCR would be combined to form the CCD
- HL7 further announced plans to work with CMS to have the CCD adopted instead of the CDA in the Claims Attachment NPRM

The White House Website Features “harmonizing standards” as a key action toward a “nationwide EHR system”

from the White House website on “Healthcare IT”
“Action: Through the President’s leadership over the past two years, the Administration has taken numerous steps towards fulfilling his health IT vision, including:

* Establishing the position of the National Coordinator for Health Information Technology within the U.S. Department of Health and Human Services (HHS);
* Providing support for several health IT projects to assess and develop solutions to key implementation issues such as:
    - o **harmonizing standards to allow different health systems to speak the same language and seamlessly share health information when needed;**
    - o developing certification criteria to ensure health IT investments meet proper standards;
    - o addressing privacy and security issues; and
    - o developing models for a national Internet-based system that allows electronic health information to follow patients no matter where they receive care

In conjunction with these efforts, the Administration has established the American Health Information Community (AHIC), a committee comprised of both public and private stakeholders called to recommend solutions to help realize the President’s goal. The AHIC is allowing major government health care players – such as the Centers for Medicare and Medicaid Services, the Department of Veterans Affairs, and the Department of Defense – to join with doctors, nurses, technology vendors, consumer organizations, insurance companies, and state and local government interests, to unify behind a common framework for implementing a nationwide electronic health records system.”

A Notice of Proposed Rulemaking (NPRM) is expected soon for Claims Attachment, which will become law 26 months thereafter

- Field tests of Claims Attachments using the CCD transmitted via EDI X12 protocols are underway
- The final CCD specification was completed March 2007, resolving all differences between the CDA and CCR (CCD=CDA+CCR)
- The HIPAA rule process, followed for all past transactions, gives a 26 month comment period after the NPRM before the rule is final
- Transactions using the Claims Attachment Rule requiring the CCD are now expected to be in wide use by 2010

Supporting the CCD and the HIPAA Claims Attachment Rule represent a requirement and a big opportunity for WorldVistA

- Unlike previous HIPAA rules, Claims Attachment can only really be done with an EHR
- Providers invested significantly to upgrade their systems to support earlier HIPAA transactions
- HIPAA Claims Attachment is likely to significantly accelerate EHR adoption
- All EHR systems will need to support Claims Attachment (in the US) by the time the Rule is final
- WorldVistA can be a viable alternative for this wave of EHR adoptions if it provides CCD and Claims Attachment support