Securing the Healthcare Enterprise: Formal Documentation and Certification Under the HIPAA Security Rule

Presentation by Jeff Jinnett, J.D., CISSP
Of Counsel, LeBoeuf, Lamb, Greene & MacRae, LLP and
President, LeBoeuf Computing Technologies, LLC

Securing the Healthcare Enterprise: The Business Perspective

- The number of reported hacking incidents more than doubled from 21,756 in the year 2000 to 52,658 in 2001
  - Source: "CERT/CC Statistics 1988-2001, Number of Incidents Reported"
- "More sophisticated technology is not the only answer. Confirming that security policies are in place and are adhered to and planning reactions to worst-case scenarios are becoming part of a new corporate mindset"
  - Source: "Feeling Insecure", Interactive Week, October 22, 2001

Securing the Healthcare Enterprise: The Business Perspective cont'd

- "Serious About Security" in the February 23, 2002 issue of Information Week reports that:
  - the Chief Security Officer job function in the financial services industry is becoming the model for the healthcare industry
  - The CSO job is being elevated to C-level status because the risks to people and data have "multiplied in complexity within just a few years"
  - 41% of CEO's are now actively involved in setting security policy
  - About 20% of Meta Group's 2,000 corporate clients have CSO's on board, and it is predicted that number will grow to 40% within 5 years

Securing the Healthcare Enterprise: The Legal Perspective

- Complex Web of Security Mandates
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - HIPAA Security Rule (Proposed)
  - Gramm-Leach-Bliley Act of 1999 (GLB)
    - Implementing security guidelines (e.g., FTC Safeguards Rule, state Department of Insurance directives)
  - Examples of other U.S. and non-U.S. privacy laws which involve security issues:
    - Federal Trade Commission Act
      - Eli Lilly case
    - U.S. Federal Sentencing Guidelines
    - State business and tort laws
    - Convention on Cybercrime
    - EU Privacy Directive

Securing the Healthcare Enterprise: The Technical Perspective – Current Information Security (InfoSec) Standards

- ISO 17799 (based on British Standard 7799)
- Common Criteria
- "Rainbow Series" (e.g., NSA Trusted Computer System Evaluation Criteria (the "Orange Book"))
- Information Technology Security Evaluation Criteria (ITSEC)
- InfoSec technical standards for digital signatures, passwords, LAN/WAN security, etc, issued by ANSI, ASTM, IETF, ISO and other standard-setting organizations
  - ASTM PS 101-97 (Security Framework for Healthcare Information)
- The proposed HIPAA Security Rule incorporates many concepts from the above InfoSec standards and expressly maps some of its mandated security implementations against 55 specific technical standards, such as ASTM PS 101-97

HIPAA Compliance Dates

- Final rules are effective 24 months after issuance in final form (or 36 months after finalization for small health plans)
- HIPAA Privacy Rule: April 14, 2003
- HIPAA Standards for Electronic Transactions Rule: October 16, 2002 (HR 3323 (Public Law 107-105) permits a one year extension to October 16, 2003 if a compliance extension plan was submitted to DHHS by October 15, 2002)
- HIPAA National Identifiers

HIPAA Compliance Dates cont'd

- HIPAA Security Rule (October, 2004 if issued in October of 2002)
  - But HIPAA act itself mandates covered entities who maintain or transmit health information to maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of the health information and to protect against security threats and unauthorized disclosures (see Section 1173(d)(2))
  - Also, security access controls are necessary in order to implement the Privacy Rule minimum necessary analysis
  - Therefore, reasonable security measures must be in place by April 14, 2003

HIPAA SECURITY RULE

HIPAA Security Rule

- Security Rule (how data is stored and accessed)
  - "procedures to guard data integrity, confidentiality and availability" applying to all individual health information in electronic form (excludes paper and oral health information); covers internal and external communications; linkage of standards and implementations in matrix; no specific technologies mandated
  - diskette, tape, CD, email, file transfer, web or EDI are included
  - telephone voice response and "faxback" systems not included

HIPAA Security Rule cont'd

- "Covered Entities" for purposes of Security Rule:
  - Health Plans (an individual or group plan that provides, or pays the cost of, medical care; includes ERISA, Medicare and Medicaid)
  - Health Care Clearinghouses (but compare definition in Privacy Rule to definition in Proposed Security Rule)
  - Health Care Providers (but only those who electronically transmit or maintain any health information pertaining to an individual)
    - other HIPAA rules apply only to providers electronically transmitting any of the covered healthcare transactions

HIPAA Security Rule cont’d

- "Each entity [subject to the HIPAA Security Rule] must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures. These measures must be documented and kept current, and must include, at a minimum, the following requirements and implementation features”:
- I. Administrative Procedures
  - Documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data

HIPAA Security Rule cont’d

- II. Physical Safeguards
  - Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion (including use of locks, keys, and administrative measures to control access to computer systems and facilities)
- III. Technical Security Services
  - Processes that are put into place to protect information and to control individual access to information
- IV. Technical Security Mechanisms
  - Processes that are put into place to guard against unauthorized access to data that is transmitted over a communications network

I. Security Standards- Administrative Procedures

- Certification/Accreditation- either internal or by third party (note possible EU Safe Harbor benefit of certification)
- Chain of Trust Partner Agreement
  - "contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged" (e.g., combination NDA/Trading Partner Agreement)
  - Combination business associate/chain of trust agreement
- Contingency Plan (<u>must include</u> applications and data criticality analysis, data backup plan, disaster recovery plan, emergency mode operation plan and testing and revision procedures)

I. Security Standards-Administrative Procedures cont'd

- Formal Mechanism for Processing Records
- Information Access Control and Personnel Security/Termination
- Internal Audit
- Security Configuration Management (e.g., virus checking), Security Management Process (e.g., risk analysis) and Incident Management Procedures (e.g., hacker response procedures)
- Initial and Ongoing Training

II. Security Standards: Physical Safeguards

- Assigned security responsibility (e.g., security management practices, assigned to specific individual or organization)
- Media controls-formal, documented procedures governing receipt and removal of hardware/software into and out of facility (must include following implementation features: controlled access to media, accountability, data backup, data storage and disposal)

II. Security Standards: Physical Safeguards cont’d

- Physical access controls (must include following implementation features: disaster recovery, emergency mode operation, equipment control, equipment control, facility security plan, procedures for verifying access authorizations before granting physical access, maintenance records, need-to-know procedures for personnel access, procedures to sign in visitors, and testing and revision)
- Policy and guidelines on work station use
- Secure work station location
- Security awareness training

III. Security Standards: Technical Security Services

- Access Control that includes
  - a procedure for emergency access to information in a crisis
  - at least one of the following implementation features: role-based access, context-based access or user-based access
  - the optional use of an encryption implementation feature
- Audit Controls (i.e., mechanisms to record and examine system activity)
- Authorization Control (i.e., mechanism to obtain consent to use or disclose PHI) that includes at least one of the following implementation features: role-based access or user-based access

III. Security Standards: Technical Security Services cont'd

- Data Authentication (i.e., corroboration that data has not been altered) by using checksums, double keying, message authentication codes or digital signatures, etc.
- Entity Authentication (i.e., corroboration that entity is the one claimed), that includes
  - Automatic logoff (query whether screen lock is alternative)
  - Unique user identification
  - At least one of the following implementation features: biometric identification, passwords, PIN's, telephone call-backs or tokens

IV. Security Standards: Technical Security Mechanisms

- For open systems, such as the Internet and dial in, apply
  - Integrity controls (i.e., internal verification that data that is being stored or transmitted is valid)
  - Message authentication (i.e., assurance that the message sent and received is the same message, typically using a message authentication code)
  - One of the following implementation features:
    - access controls (i.e., dedicated, secure communications lines); or
    - encryption

IV. Security Standards: Technical Security Mechanisms cont'd

- In addition, if using a network for communication, use:
  - Alarms (e.g., device that senses abnormal condition)
  - Audit trails (data collected and potentially used for security audit)
  - Entity authentication
  - Event reporting (e.g., network message indicating operational irregularity in physical elements)

Use of Encryption

- Encryption Required for PHI Transmitted Over Public Networks (dial-in, wireless and Internet, including emails sent and received over the Internet)
- Encryption Optional for Networks Protected by Access Controls (e.g., value-added networks (VAN’s) and private wire, dedicated networks, including intranets)
- Control over Media (electronic storage mechanism) required (e.g., physical control over device and access control over data and/or encryption of data)

Use of Encryption cont'd

- For Data Transmission, Provide for Integrity Checking and Entity Authentication (e.g., if received unencrypted email from patient with PHI, call patient back to confirm identity and authenticity of PHI; preferable to establish secure sockets layer connection to patients in order to authenticate patients and encrypt emails)
- Note that individual health information must be maintained as secure not only while in transmission, but also while at rest (this differs from the HCFA/CMS Internet Security Policy): therefore, disable batch email forwarding to employees' homes when they are out of the office, if the emails may contain PHI; also consider encrypting PHI on laptops and PDA's

Security Hypotheticals

- PHI + Speech or Paper: no application of HIPAA Security Rule, but HIPAA Privacy Rule still applies
- PHI + Text + Phone Lines (Using Modems): all HIPAA security requirements, except encryption
- PHI + Text + Air (Short Distance, With Low Chance of Interception): all HIPAA security requirements, except encryption
- PHI + Text + Ethernet (With Poor Access Control): all HIPAA security requirements, including encryption
- PHI + Text + Air (Long Distance, With Definite Possibility of Interception): all HIPAA security requirements, including encryption
- Essentially, if interception of an electronic message is a definite possibility, then encryption is required

Mapped Technical Standards

- The HIPAA Security Rule is intended to be comprehensive, technology-neutral and scalable (i.e., less is expected from a small, rural covered entity than from a major covered entity)
- The four categories of mandated security requirements and mandatory and optional security implementations map against 55 technical standards, issued by the following standard-setting organizations: ANSI, ASTM, CEN, FDA, FIPS, IEEE, IETF, ISO/IEC, NIST, PKCS, RFC

Mapped Technical Standards cont'd

- For example:
  - the certification requirement under Category I maps against the NIST "Generally Accepted Principles and Practices for Secure Information Technology Systems"
  - The data authentication requirement under Category III maps against ASTM E 1762 "Standard Guide for Authentication of Healthcare Information" and Computer Science and Telecommunications Board, For The Record-Protecting Electronic Health Information (1997)

Electronic Signatures

- Proposed Security Rule does not mandate use of electronic signature, but if one is used, the following three implementation features must be implemented:
  - Message integrity
  - Non-repudiation
  - User authentication
- electronic signature standard applies only to covered transactions (see HIPAA Standards for Electronic Transactions Rule)
- Only the digital signature form of electronic signature is approved in rule for use
- In final Security Rule, electronic signature provisions may be deleted and a separate electronic signature rule may be issued

Certification

Security Rule Certification Requirement

- DHHS: “Each organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency. We are, at this time, soliciting input from...independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance....”

Board of Directors Duty of Care and Application of the Business Judgment Rule

- Under state law, directors are expected to perform their duties with due care and to be reasonably well-informed when making decisions, taking the best interests of the corporation into account
- In many states, so long as the directors acted with due care, they are not personally liable unless they are guilty of gross negligence or willful misconduct
- If directors fail to act with due care, they can be held liable if only guilty of simple negligence
- For public companies, due diligence record can help establish defense under securities laws

HIPAA Criminal and Civil Penalties

- Federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose protected health information or obtain protected health information under false pretenses and for knowing misuse of a unique health identifier:
    - Criminal penalties of up to $50,000 and one year in prison for obtaining or disclosing protected health information
    - Criminal penalties of up to $100,000 and up to 5 years in prison for obtaining protected health information under "false pretenses”
    - Criminal penalties of up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.
- For violations of transaction standards, penalties of up to $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year.

Need for a HIPAA Due Diligence Record

- HIPAA due diligence record satisfies requirement under Security Rule for a certification as to compliance, with supporting documentation
- Due diligence record made a part of periodic reports to the Board of Directors establishes a business judgment rule defense
- Due diligence record helps establish defense against criminal proceedings by establishing that no “knowing and improper” actions on the part of corporate officials are involved
- Although accreditation agencies are not HIPAA enforcers, they may in the future decide to incorporate some HIPAA standards into their accreditation process (e.g., Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and the National Committee for Quality Assurance (NCQA))

Due Diligence Record Also Serves as a Risk Mitigation Plan

- Ensures that the enterprise HIPAA project is correctly prioritized from a technical, business and legal point of view in case a significant percentage of the enterprise cannot be brought into compliance by the deadline
- "Bottlenecks" are identified which could delay full and timely project compliance
- Industry "best practices" are identified and matched to the company's HIPAA plan

Obtain Third Party "Certifications"

- Independent HIPAA certifications
  - Electronic Healthcare Network Accreditation Commission (EHNAC) Security Accreditation
  - audit by outside HIPAA consultant
  - legal review of HIPAA interpretation (e.g., memorandum of law to support interpretation of compliance with de-identification "safe harbor", combined with statistical expert report)
  - Qualification for HIPAA insurance (e.g., Chubb Executive Risk endorsement to D&O policy)
  - Seek to have Company's approach cited in publication as example of "best practices"
  - SAS 70 or comparable audit

Identify “External Validators”

- Identify any listserv submissions (e.g., Hipaadvisory and WEDI) which support enterprise’s HIPAA security approach
- Match enterprise approach against industry guidelines (e.g., HIPAA Security Summit Guidelines or the Association of American Medical Centers Guidelines for Academic Medical Centers on Security and Privacy)
- Compare enterprise project status to peer companies as reported in healthcare industry HIPAA status surveys (e.g., Gartner Group and First Consulting Group)

Identify “External Validators” cont’d

- Compare enterprise definitions of internal and external risk against industry definitions (e.g., AFEHCT Security Best Practices Proposal)
- identify external validators for assessment, remediation and testing tools used (e.g., SEI Octave risk assessment methodology, WEDI Standard National Implementation Process (SNIP) Security and Privacy Workgroup White Paper or the CPRI Toolkit: Managing Information Security in Health Care)
- review special security issues (e.g., email security) against industry white papers (e.g., AHIMA email white paper)

Securing the Healthcare Enterprise: An Enterprise Process Management Challenge

- Cost of HIPAA compliance and Solution Approach
  - 3 to 4 times the information technology (IT) cost of Y2K (Fitch Report, "HIPAA: Wake-UP Call for Health Care Providers")
  - Although the bulk of the cost will be in IT remediation, only 30% of HIPAA impact will be on IT, while 70% of impact will be on business processes (Lee Barrett, WEDI and EHNAC)
  - Therefore, an enterprise process management (EPM) approach is better suited to HIPAA than a pure IT-driven approach

Conclusion: Institute and Maintain an Enterprise Process Management Approach in Order to Secure Your Healthcare Enterprise

- Avoid fragmented HIPAA project teams, where issues can fall between the cracks
- Don’t lose the forest for the trees
- Map the enterprise business processes and existing IT infrastructure security features against the mandated security requirements
- Identify third party certifications as to “best practices” and external validators which match your project approach
- Document compliance with security mandates and keep the formal documentation updated
- Produce a summary due diligence document which can be produced to explain your security approach