HIPAA Summit West

Accrediting and Certifying Security Policies and Enforcement Programs Under HIPAA

Richard D. Marks

Davis Wright Tremaine LLP

Washington, D.C.

Seattle, Portland, San Francisco, Los Angeles, Anchorage, Honolulu

New York, Charlotte,

(202) 508-6611

richardmarks@dwt.com

Copyright 2001 Richard D. Marks

All Rights Reserved

"Certification" in HIPAA's Proposed Security Rule

1. What does "certification" mean in this context?
2. How is it done?
   - What standards?
   - How often?
   - What's the product or outcome?
   - Who does it?
   - Where or what does it get you?
   - What does it cost?
3. What must you do once you've been certified?
4. Are there liability issues?

Proposed Security Rule

Security Standard

- "Comprehensive adoption of security standards in health care, not piecemeal implementation, is advocated to provide security to data that is [*sic*] exchanged between health care entities."
- HIPAA Security Matrix, containing:
  - "Requirements"
  - "Implementation Features"

Proposed Security Rule

Security Standard

"We would define the security standard as a set of requirements with implementation features that providers, plans, and clearinghouses *must* include in their operations to *assure* that electronic health information pertaining to an individual remains secure." (Emphasis added.)

Proposed Security Rule

Security Standard - Specific Requirements

"The proposed security standard consists of the requirements that a health care entity *must* address in order to safeguard the integrity, confidentiality, and availability of its electronic data. It also describes the implementation features that *must* be present in order to satisfy each requirement." (Emphasis added.)

Administrative Procedures

- ✓ **We would require <u>each</u> [administrative requirement and supporting implementation feature] to be <u>documented</u>. . . .[and] to be made available to those individuals responsible for implementing the procedures and would require [the documentation] to be <u>reviewed and updated periodically</u>."**
- ✓ ***Certification is the first-listed requirement. NO implementation features were proposed.***

Administrative Procedures - Certification

"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."

Administrative Procedures - Certification

Questions:

- Is certification related only to computer system(s) or network design(s)?
- What happens when those systems or designs change (as happens continuously)?
- To what extent will the business processes related to operation of computer systems and networks be implicated in the certification process?
- How do these issues relate to industry standards or best practices (the industry standard of care)?

Proposed Security Rule - Certification

"We are . . . soliciting input on appropriate mechanisms to permit independent assessment of compliance. We would be particularly interested in input from those engaging in health care electronic data interchange (EDI) as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation."

Proposed Security Rule - HIPAA Glossary

Certification:

"The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design *and implementation* meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency."

Proposed Security Rule - HIPAA Glossary

Certification (additional definition):

"Part of administrative procedures to guard data integrity, confidentiality, and availability."

Interpretation

"*Implementation*" covers much more than

- ✓**Computer system and network design**
- ✓**Testing and validation of system changes**
- ✓**Certification of off-the-shelf products**

"*Implementation*" (in computer security usage) covers the range of policies, processes, and procedures in the <u>installation and operation</u> of computing and telecommunications facilities. Good implementation avoids creating, or failing to detect existing, *specific vulnerabilities.*

“Specific Vulnerability”

- A weakness in a system that allows it to be compromised. The weakness may be in the
  - System’s original design
  - Subsequent changes to the system (necessitates change control)
  - How the system is operated as a matter of policy, or in fact

HIPAA Security Change Control

Security Configuration Management **(a requirement under Administrative Procedures - this is change control)**

The organization would be required to implement measures, practices, and procedures for the security of information systems. These would be coordinated and integrated with other system configuration management practices in order to create and manage system integrity. This integration process is important to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses. (continued)

HIPAA Security Change Control

Security Configuration Management

(continued) The requirement would include the following:

- Documentation
- Hardware/ software installation and maintenance review and testing for security features.
- Inventory procedures.
- Security testing.
- Virus Testing.

Questions

1. What standards do the HIPAA Security Rules mandate or suggest for evaluating covered entities' systems and their implementation?

   Note: Standards listed in proposed security rule are "mapped" to matrix "requirements" and "implementation features" (Addendum 3)

2. What comparable evaluation standards exist in other areas?

Generally Accepted Accounting Principles (GAAP)

The standard under which are performed:

- **Financial accounting**
- **Financial auditing**

FASB - Financial Accounting Standards Board - independent body - recognized as authoritative under:

- **SEC Financial Reporting Release No. 1**
- **AICPA Rules of Conduct, Rule 203**

Electronic Healthcare Network Accreditation Commission (EHNAC)

The Electronic Healthcare Network Accreditation Commission is an independent, not-for-profit accrediting body. It is comprised of an Executive Director and no less [*sic*] than nine (9) industry and consumer representatives.

EHNAC has 2 accreditation programs:
EHNAC Healthcare Network Accreditation
EHNAC Security Accreditation

ANSI

American National Standards Institute

The American National Standards Institute (ANSI) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 80 years. Founded in 1918 by five engineering societies and three government agencies, the Institute remains a private, nonprofit membership organization supported by a diverse constituency of private and public sector organizations.

ISO
IEEE

- International Organization for Standardization
- Institute for Electrical and Electronic Engineers (I-triple-E)
- Both issue standards.

American Society for Testing and Materials

Standards for Security and Electronic Signatures in Healthcare (1999)

- Very detailed provisional standards cover security implementation generally, and subtopics such as PKI and access
- Are these standards affordable, and is mature technology available to implement them, in healthcare in the next 2 years? (Probably not!)

JCAHO

The Joint Commission will assess the implications of this new regulation [the HIPAA final privacy rule] for its standards and the accreditation process to determine if changes are necessary. While the Joint Commission supports the goals of HIPAA, it is essential that those involved in caring for patients have appropriate access to medical information about those patients to optimize the provision of safe and effective care and to identify and assess opportunities for improving the quality and safety of patient care.

NCQA

NCQA is an independent, non-profit organization whose mission is to evaluate and report on the quality of the nation's managed care organizations.

Information Systems Standards: NCQA has delayed introduction of IS standards in view of upcoming federal regulations on data security and confidentiality, as provided for in the Health Insurance Portability and Accountability Act (HIPAA).

National Institute of Standards and Technology (NIST)

** The purposes of [the Computer Security Act of 1987] are--
(1) . . . .to assign to [NIST] responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate . . . .

** Publishes the "Common Criteria for Information Technology Security Evaluation"

-- Very detailed

-- Largely unknown in healthcare (implications for HHS?)

AICP/ CICA
WebTrust™ Program for Certification Authorities

- Version 1.0., Aug. 25, 2000
- Applies to e-commerce functions of CAs and RAs using PKI systems (digital signatures)
- A means for relying parties to know that another individual's or entity's public key actually belongs to the person/ entity
- WebTrust™ seal program
- Examination standards (U.S.): Statements on Standards for Attestation Engagements
- Disclosure criteria derived from ITEF Internet X.509 PKI Certificate Policy

ABA Section of Science & Technology Law: *PKI Assessment Guidelines*

- In advanced drafting stage now
- Very detailed & sophisticated
- Offers context for PKI implementation that is very useful for practical security programs generally, *i.e.*, the background discussion goes beyond encryption
- No date yet for initial public issue

Certification - Questions of Scope

What gets certified? Some possibilities:

- PKI implementation alone
- Policies and procedures (administrative security) (eg, access restrictions; level of surveillance)
- Physical security
- Personnel security
- Business associate contract security issues
  - Adequacy of contracts
  - Covered entity's
    - Knowledge of BA's security means (triple-edged!)
    - Surveillance of BA's compliance (reg v. tort standard)
- Total implementation package

HIPAA - Statutory Standard

"Each person … who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards --

(A) to *ensure* the *integrity and confidentiality* of the information; and

(B) to protect against *any* reasonably anticipated

(i) threats or hazards to the *security or integrity* of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) *otherwise to ensure* compliance with this part by the officers and employees of such person."

(42 USC §1320d-2(d)(2); in effect now - does not require final security or privacy rules to become effective)

What is the industry standard of care?

- The HIPAA security rules were abstracted from the defense establishment. The abstraction is now being imposed on health care.
- So the industry frame of referenced is the military-industrial complex.
- The certifying authority for the security of the defense establishment's systems (and system implementation) is the National Security Agency.
- There is no comparable standards-setting authority for health care systems.

HIPAA Context

- ✓ Enforcement - litigation-operational perspective (*e.g.*, malpractice)
- ✓ Civil penalties (42 USC §1320d-5) - HHS/ OCR
  - $100 each violation (transaction costs)
  - $25,000 annual limit for violating each "identical requirement or prohibition" - could be a big number
- ✓ Criminal penalties (42 USC §1320d-6) - DOJ/ U.S. Attorney
  - Knowingly - 1 year/ $50,000
  - False pretenses - 5 years/ $100,000
  - Malice, commercial advantage, personal gain - 10 years, $250,000
- ✓ Private law suits by patients
  - Easier because standard of care is so much higher
  - Statute trumps the regs: "***any*** reasonably anticipated," "ensure"
  - Best practices - what is "any reasonable"? References are security processes and technology in ***defense*** (and in the ***financial***) industry

Certification by an Outside Entity

Consulting or Accounting Firm

- What standard will they use?
  - Mapped standards in HIPAA?
  - ABA Section of Science & Technology Law - PKI Assessment Guidelines ?
  - Negotiated standards with client?
  - Lawyers' role in defining standard of care *and* responding to auditors' requests for information (FASB 5)
- What procedure or protocol? (Whose best auditing practices? Like a GAAP-based audit?)
  - AICPA Auditing Standards beyond WebTrust (for CAs)?
- What will they certify?
  - The system at a moment in time!
  - Any change invalidates the certification, or at least casts it into doubt!
  - Will they - can they - arrange to certify changes in system configuration or operating procedures?

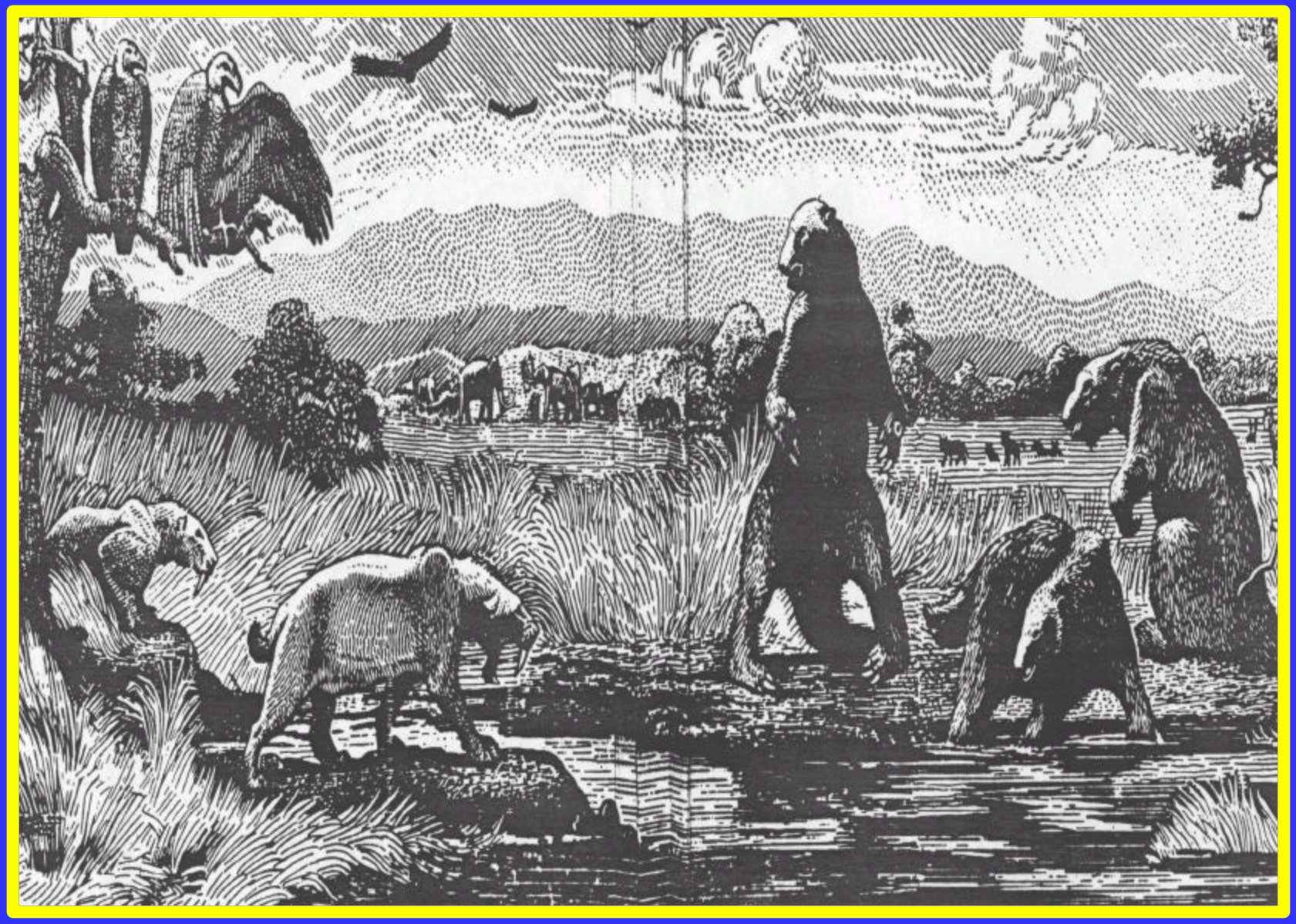
Certification by an Outside Entity

Consulting or Accounting Firm

- What are the liability issues?
  - Compare to auditors' liability in the securities field
  - Necessity for the auditors to
    - Tightly circumscribe their opinions
    - Seek the *client's* indemnification for improper use of the certification (use outside agreed-upon scope)
  - These limitations will slowly evolve into industry-standard practices
    - Will HHS seek to regulate these practices, mirroring the SEC?

Certification by the Covered Entity Itself

- Same issues regarding:
  - Standard to use in the certification "audit"
  - Procedure or protocol of the certification process
  - Continued validity of the certification as the system and operating procedures are changed
- New issue: inherent conflict of interest
  - Inevitable bar?
  - Management pressure?
  - How shield within organization?
  - How supplement (*e.g.*, outside entity hired to perform periodic penetration exercises)?
  - Litigation considerations?
- Will HHS condition acceptance (how)?
- Possible advantage: control the standards



Summary - HIPAA Certification Today

- At the moment, a tar pit, or a swamp waiting to be drained; as with much of HIPAA, the implementation details are enormously complex and uncharted.
- The standards that might be transferred from the defense and financial industries are far stricter than anything in health care.
- The security certification (and accreditation) standards for HIPAA's covered entities (and business associates) are nascent.
- You can waste a great deal of money with consultants or auditors if you fail to define the legal and operational standards they will use.
- There are indeed liability issues - be careful!
- WEDI.org > Privacy & Security > Certification White Paper