HIPAA Basics: The Privacy Manual, Litigation Risks and Business Associates

Richard D. Marks

Keith M. Korenchuk

Davis Wright Tremaine LLP

Washington, D.C.

Seattle, Portland, San Francisco, Los Angeles, Anchorage, Honolulu, New York, Shanghai

richardmarks@dwt.com

keithkorenchuk@dwt.com

Hypothetical for Analysis

- University of Washington facts
  - 4,000 complete records hacked
  - Hacker: I did it just to show you how bad your security is - a warning
- Suppose another hacker attacks you and posts 1,000 records to the Internet
  - What's the liability?
  - How could you have limited exposure?
  - How do you defend?
  - How do you mitigate?

Hypothetical for Analysis

- University of Montana facts
  - No hospital at University of Montana
  - Grad student in psychology does research at children's hospital in St. Paul, Minnesota
  - 400 pages of PHI (psych records of 62 children) is sent back and posted on University's intranet (password protection)
  - Search engine leads directly to the URL
- Suppose your researchers do this?
  - What's the liability?
  - How could you have limited exposure?
  - How do you defend/ mitigate?

Hypothetical for Analysis

- University of Minnesota facts
  - 410 deceased organ donor identities revealed to recipients
  - Second breach in 90 days
- Suppose your facility made 2 errors within a short period of time?
  - How do you defend the second incident?
  - How do you make improvements?

Hypothetical for Analysis

- Eli Lilly
  - Releases e-mail addresses of 669 Prozac patients
  - Patients receive e-mail reminding them to take their medication, but in notice to them all addresses disclosed
- FTC Investigation and Settlement
  - Lilly must establish better safeguards
  - Subject to future fines for noncompliance
- Lesson for covered entities?

Potential Civil Liability - Ratcheting Duty of Care

Tort - Negligence

Tort - Invasion of Privacy

Publication of Private Facts

False Light (akin to Defamation)

Unauthorized Commercial Use

Tort - Breach of Confidence (Physician-Patient)

Tort - Defamation

Tort- Fraud

Statutory - Consumer Fraud

Contract - Breach of Confidentiality Clauses/Policies

Contract - Breach of Express or Implied Warranty

Contract - Suits by Business Associates

Contract - Suits by Vendors/ Customers (& vice versa)

Employment -related suits (HIPAA sanctions issues)

What Does the Law "Know" About HIPAA?

- Statutes and administrative regulations (*e.g.*, transaction sets, privacy, security rules) are laws
  - Epidemic of complexity
  - Ambiguities abound
  - Initial interpretation of complexity and ambiguity in laws requires legal reasoning
- What guidance for the lawyers?
  - No litigation yet, so no decided cases
  - Supreme Court in *Mead*: can't rely on informal administrative guidance

HIPAA - Statutory Standard

"Each [covered entity] … 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)

The Ratcheting Legal Standard

The T.J. Hooper case

- New Jersey coast (1928) - storm comes up, tug loses barge and cargo of coal
- Plaintiff barge owner: captain was negligent because he had no weather radio
- Learned Hand, J.: Barge owner wins
  - Rationale: to avoid negligence, keep up with technological innovations - they set the standard of care in the industry

What is the standard of care?

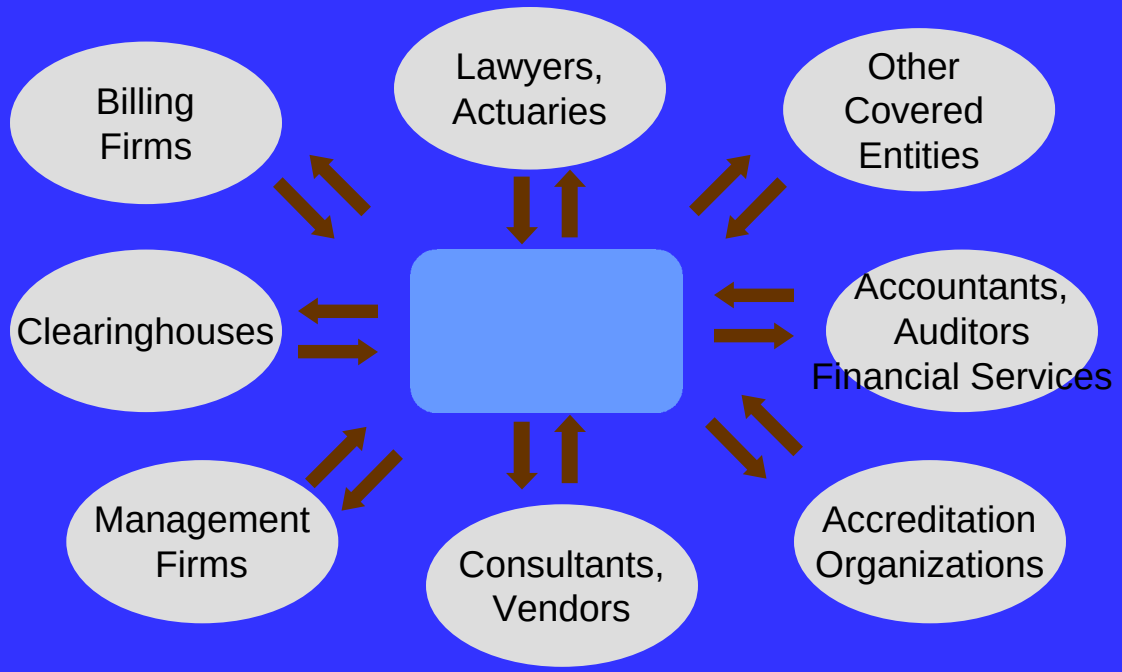
- The HIPAA security rules were abstracted from the defense establishment. The abstraction is now being imposed on health care.
- So the industry frame of referenced is the military-industrial complex, where NSA sets the rules.
- The financial industry also offers a frame of reference.
- These industries have been working for a long time on security, and have notably different structures and missions from health care.

Risk Management Analysis

- ✓ Does meeting the [proposed] regulation satisfy the HIPAA statute (reasonable and appropriate safeguards to ensure/ protect against any reasonably anticipated threat, hazard, or unauthorized use)?
- ✓ Does meeting the [proposed] regulation satisfy state tort law duties of prudent care?
- ✓ Examples: internal email; internal storage; remote use policies

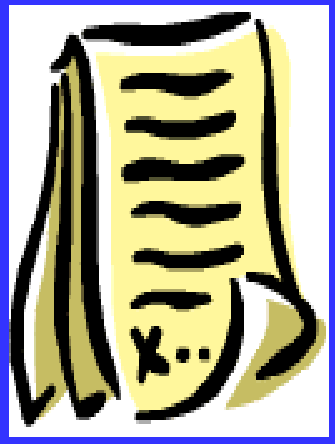
Use and Disclosure — Who Is a Business Associate?

- ✓ A person who receives individually identifiable health information and
- ✓ On behalf of a covered entity performs or assists with a function or activity involving use or disclosure of information or otherwise covered by HIPAA or provides certain identified services to a covered entity
- ✓ May be a covered entity



Use and Disclosure — Business Associate Contracts

- ✓ A covered entity may disclose protected health information to business associates if:
  - ✓ Obtains "satisfactory assurance" that business associates will appropriately safeguard the information
- ✓ Business associate contract required



Business Associate Agreements

BAA between covered entity and BA - BA must:

- ✓ Use appropriate security safeguards
- ✓ Report any improper use or disclosure *of which it becomes aware* to the covered entity
- ✓ "Ensure" its agents (including subcontractors) agree to same restrictions as in the BAA
- ✓ How much must you -- should you -- know about the security systems of your business associates?
  - ✓ If you deliberately don't ask for all details, what legal promises and assurances should you ask for?

Business Associates Liability Issues

- ✓ Privacy Rule, 45 CFR § 164.504(e)
  - ✓ "[W]e have eliminated the requirement that a covered entity actively monitor and ensure protection by its business associates." 65 *Fed. Reg.* 82641.
  - ✓ However: "Covered entities cannot avoid responsibility by intentionally ignoring problems with their contractors."
- ✓ The big question: What about duties under state tort law?
  - ✓ Prudent behavior standard
  - ✓ Enhanced by the HIPAA statutory standard?

Covered Entity - Vendor/ Business Associate Contract Negotiations - Litigation Risk Management

- A new set of risks for both sides
- No vendor is "HIPAA compliant," because the security is in the implementation. Only covered entities (and business associates) can be HIPAA compliant.
  - Some systems are just easier to engineer into a secure implementation -- and some can't be engineered that way as a practical matter.
  - Business process + technology = security
- Health care IT system vendors will ask for indemnification from covered entities against weak implementation.
- Will the provider community resist or cave in?

Enterprise Compliance Plan for Information Security

Achieving a reasonable level of security is a multifaceted task

+ Initial and on-going threat assessment (outside experts) >> enterprise security process
  + Computer security
  + Communications security
  + Physical security: access to premises, equipment, people, data
  + Personnel security
  + Procedural (business process) security
  + A pervasive security culture

"Effective program to prevent and detect violations of law"

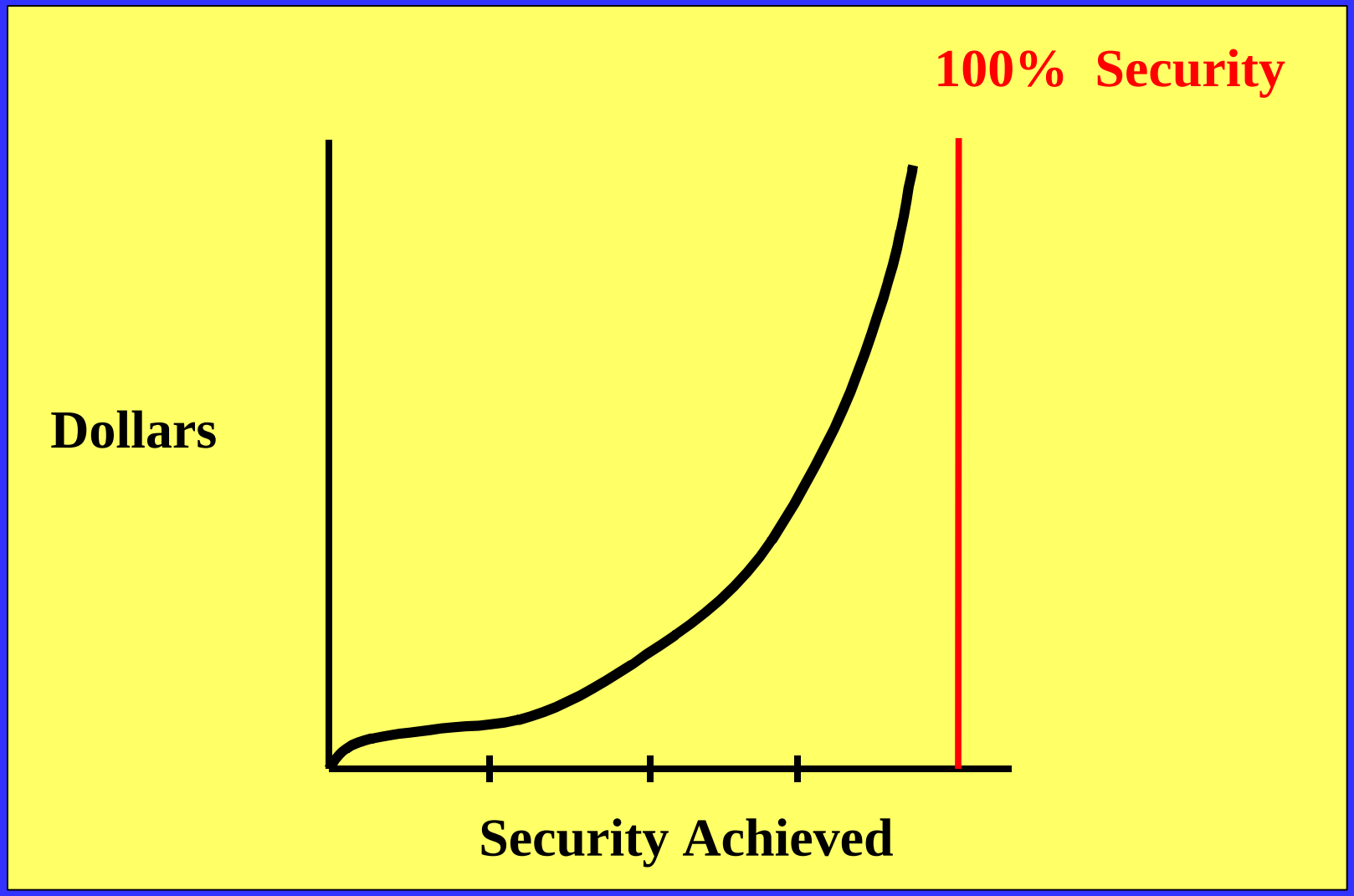
- ✓ Establish compliance standards
- ✓ High-level personnel must have been assigned overall responsibility
- ✓ Due care not to delegate substantial discretionary authority to those with propensity for illegal activity
- ✓ Effective communication of standards
- ✓ Reasonable steps to achieve compliance with standards
- ✓ Standards consistently enforced through appropriate disciplinary mechanisms
- ✓ All reasonable steps to respond once an offense is detected (including preventing further similar offenses)
- ⌗ Same principles as Business Judgment Rule (insulating corporate officers and directors from personal liability)

Expense v. Security Achieved

Expenditure compared to security achieved is not a linear relationship; it becomes geometric, then exponential, and is always asymptotic.

- **E.g.:**
  - **60% security = $ 1 million**
  - **80% security = another $ 2 million**
  - **95% security = another $ 4 million**
  - **etc.**
- **Budget issues are a major element of litigation risk management - you are dealing with the art of the practical**

Expense v. Security Achieved



Finally

- Security is a goal, a process, and a state of mind, not a steady state or a product.
- Technology is but a small part of security - and it must be implemented securely within the institution's business and clinical processes.
- Transaction & Code Set and Privacy rules are implemented within the framework of Security.
- The statute and rules are loaded with ambiguities.
  - Interpretation of the ambiguities and examination of options can't be done without legal analysis.
  - What other "law" bears on the issue?
  - Litigation risk analysis informs the risk-taking inherent in HIPAA-related business decisions.