

**The HIPAA Colloquium at Harvard University**

**Legal Issues in HIPAA  
Security Compliance**

**Richard D. Marks**

**Davis Wright Tremaine LLP**

**Washington, D.C.**

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

**(202) 508-6611**

**[richardmarks@dwt.com](mailto:richardmarks@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 a hacker attacks your plan and posts 4,000 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 staff has a lapse like 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 plan 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

## ⇒ Settlement with states: \$160,000

## ⇒ Lesson for Covered Entities and Bus. Assocs.?

# 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)

# 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)

# HIPAA Context

- ✓ **Enforcement - litigation-operational perspective (e.g., malpractice) -- HHS enforcement is least of worries**
- ✓ **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**
- ✓ **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**



# **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)**

# Security

**When does it apply?**

**What's its scope?**

- **Wrong answer**: 26 months after final security rule appears in Federal Register
- **Immediate concern**: 42 USC §1320d-2(d)(2) applies now to “health information”
- **45 CFR §164.530(c)** requires appropriate security measures when the privacy rules are implemented on April 13, 2003 (brings application of the final security rules forward)

# **Privacy Rule Requirements for Security**

## **45 CFR 164.530 (c)**

**Existing: “A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”**

# **Privacy Rule, 45 CFR 164.530 (c)**

**Existing: “A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.”**

# **Privacy Rule, 45 CFR 164.530 (c)**

**New: “A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.”**

# **Privacy Rule, 45 CFR 164.530 (c)**

**New in Preamble: “[A]n incidental use or disclosure is permissible only to the extent that the covered entity has applied reasonable safeguards as required by § 164.530 (c) and implemented the minimum necessary standard . . . .” 67 Fed. Reg. 53193-94.**

# **Privacy Rule, 45 CFR 164.530 (c)**

**New in Preamble: “[T]he Privacy Rule applies to protected health information in all forms [oral, written, or other electronic forms], [and] the Security Rule will apply only to electronic health information systems that maintain or transmit individually identifiable health information.” 67 Fed. Reg. 53194.**

# Privacy Rule, 45 CFR 164.530 (c)

- ✦ Confirmation of a significantly expanded reach for security principles
- ✦ What sources will be used to interpret “reasonable safeguards” under § 164.530(c)? (Think like plaintiff’s counsel.)
  - ✦ The statute: 47 USC § 1320d-2 (d)(2)
  - ✦ The security rule when published in final form
  - ✦ The bibliography of the proposed security rule (can’t undo history)



# Chain of Trust

**“A chain of trust partner agreement (a 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).”  
Proposed §142.308, 63 Fed. Reg. 43266.**

**“The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. . . . so that the same level of security is maintained at all links in the chain . . . .”  
63 Fed. Reg. 43252.**

# 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's Different After Sept. 11?

- ❖ Security is no longer
  - ❖ in the background
  - ❖ abstract
  - ❖ unfamiliar
- ❖ In government and industry, executives are placing a priority on reviewing security (threat and response models)
- ❖ Health care entities must contemplate security threat and response models, and their human, business, and legal consequences
- ❖ We are obligated to think about providers as a potential terrorist delivery system, like airplanes and mail (plans and clearinghouses do not want to be a back-door source into providers' systems)

# There Are Threats

- \* Hackers & Crackers
- \* Industrial/Corporate Spies
- \* Trusted Insiders
  - \* Employees
  - \* Consultants
- \* Organized Crime
- \* Terrorists



# You Will Suffer a Security Breach

- **Either Internal or External, but...**
- **It doesn't have to be devastating**
- **Create an Information Security Policy**
- **Create an Incident Response Plan**
  - **Media Issues**
  - **Mitigation**
  - **Preservation of Evidence**
- **Implement Security Safeguards**

# **Criminal Law - Federal Sentencing/Prosecution Guidelines - Relationship to Business Judgment Rule**

**Structured approach - covers organizations**

**Why? Because HIPAA violations can be criminal.**

**Some definitions from Sentencing Guidelines:**

**“High-level personnel of the organization”**

**“Substantial authority personnel”**

**“Condoned”**

**“Willfully ignorant of the offense”**

**“Effective program to prevent and detect violations of law”**

# **“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)**

# Litigation & Operational Perspective

- ◆ What new operating policies must we prepare?
  - ◆ *These policies are legal documents that will be of utmost importance in litigation*
- ◆ What records must we keep to
  - ◆ Cooperate with HHS?
  - ◆ Defend ourselves in state or federal court?
    - ◆ Civil
    - ◆ Criminal
- ◆ How do these records requirements translate into audit trails? (Complying with the Privacy and Security rules demands automation.)
- ◆ Can our installed systems accommodate these audit trail and related access requirements? What are other elements of compliance?



# Case to Consider

*U.S. v. Mead Corp.* (U.S. Sup. Ct. No. 99-1434, June 18, 2001)

© Customs Service ruling letters about tariff clarifications – was it authoritative?

© Answer: NOT authoritative, because not a:

© Notice and comment rule making (formal proceeding), or

© Administrative adjudication

© Consequence: weight of informal agency guidance depends on how good the reasoning is (persuasive?)

© So can't rely on HHS's informal guidance for HIPAA – it may not be authoritative

# Business Associates

- ✓ **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?**

# Remote Use - Security Breaches

THE WALL STREET JOURNAL

## MARKETPLACE

Advertising: *Mattel's Barbie brand wants to start targeting mothers* Page B8.

Career Journal: *Some online job sites try offering sweepstakes* Page B16.

### redit-Card Scams Bedevil E-Stores

*No Signatures to Prove Who Placed Orders, Sites re Left Footing the Bills*

By JULIA ANGEVIN  
*Reporter of THE WALL STREET JOURNAL*

STEPHEN LIKE a valid order. A customer calling herself Arina Hadir visited Victor Stein's Web site in April and ordered a \$700 collector's edition of The Beard Encyclopedia, which Mr. Stein ordered.

When the transaction was authorized by Mr. Stein shipped the book to an address never provided by the customer and he no more about it. After all, says the New York sugar broker who writes about himself on the side, 25% of his sales come from bilious enthusiasts.

Two months later, Mr. Stein found out a way that credit-card fraud is a growing problem for Internet merchants. Account documents provided by Mr. Stein, did claim to Visa a few weeks later a hadn't ordered the book. She also did a number of other items on her bill had been ordered from other Web sites, eg Amazon.com. So at the request of Visa's credit-card issuer, Mr. Stein's Chase Manhattan Corp., took the bill out of his account to reimburse the Credit Commercial de France, for its bill to Mr. Stein.

He noted that Visa had authorized the card transaction and that Mr. Stein could



### A Stolen Laptop Can Be Trouble If Owner Is CEO

By NICK WINGFIELD  
*Staff Reporter of THE WALL STREET JOURNAL*

Iris Jacobs came face-to-face with one of the biggest security issues facing American business executives these days: What happens when a laptop chock full of business secrets gets ripped off?

Mr. Jacobs, the chief executive and founder of Qualcomm Inc., had his laptop stolen from a journalism conference this past weekend in Irvine, Calif. The IBM ThinkPad laptop, which he had used to give a presentation at the conference, contained megabytes of confidential corporate information dating back years, including financial data, e-mail and personal items.

The theft was a painful reminder of one of the unforeseen costs of the New Economy's most powerful tools: new portable technologies like laptop computers, hand-held electronic organizers and cellular phones. While the devices offer unprecedented flexibility to executives, they also lead to frightening lapses in information security because of the sheer volume of data that can be hauled around on them.

Basically, business data have moved from paper to digits, but many companies aren't moving as quickly to update their security measures. Laptop theft, in particular, is "a big issue—it cuts across all different types of companies," says Richard Heffernan, a security consultant with R.J. Heffernan Associates Inc. in Bradford, Conn., which performs security audits and other services for large corporations.

Some firms are being careful to protect sensi-

# Wireless Devices

## ⚡ Extremely useful for

- ⚡ Patient care
- ⚡ Transcription
- ⚡ Order entry
- ⚡ Remote consults
- ⚡ HIPAA administrative issues

## ⚡ Security issues

- ⚡ Intercepts - encryption helps a great deal
- ⚡ Lost (or stolen) on the [subway] - physical access
- ⚡ Authenticating access

## ⚡ DOD/ NIST: Restrictions on wireless LANS

- ⚡ Intercepts (1,000 feet minimum)
- ⚡ No true access port authentication (IEEE 802.11/802.11b)

# Authenticating Access is a Separate Set of Risk Management Issues

⌚ How do you control who is really using the key to which the digital certificate relates?

- Password alone fails the industry standard of care

- Password (PIN) plus

  - Secure ID?

  - Smart Card?

  - Biometrics (probably part of the eventual answer)

- Emergency access

⌚ How do you pay to administer all this?

Industry experience: costs rise steeply well before 1,000 cards, tokens, or whatever

# **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**
- ⊗ **IT system vendors will ask for indemnification from covered entities against weak implementation.**
- ⊗ **Will the provider community resist or cave in?**

# PKI in the Real World

- ⊗ Verisign issuance of 3 spoofed certificates for use on MSN. Question: how many others?
- ⊗ Same facts at hospital, plan, or clearinghouse:
  - ⊗ Could not trust anything on the system.
  - ⊗ Must you take the whole system down?
  - ⊗ If so, how do you function? Dangers (malpractice)?
  - ⊗ Regulatory review?
  - ⊗ Impact on public and customer relations?
- ⊗ What's the systems answer in managing risk?
  - ⊗ Constant hot backups?
  - ⊗ With ongoing integrity checking and encrypted storage?
  - ⊗ Where would you buy that?

# Business Associate Agreements

## BAA between covered entity and BA - BA must:

- ✓ Not use or further disclose the PHI other than as
  - ✓ Permitted in the BAA or
  - ✓ As required by law
- ✓ Use appropriate security safeguards (think chain of trust)
- ✓ 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
- ✓ Make available to HHS its internal practices and books relating to use and disclosure of PHI
- ✓ 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?



# 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.”

# General Rule

**Research + PHI = HIPAA  
Authorization**

# Disclosing PHI to a Research Database

- If authorization is required, expiration date may be “none”
- What is the disclosing entity’s risk under
  - the HIPAA statute?
  - the security rules (in final form) (think chain of trust)?
  - state law?

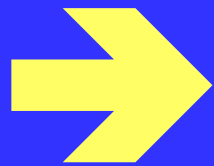
# OHCAs

- ❑ Rules for operation among participating Covered Entities and their Bus. Assocs.
- ❑ OHCAs will use integrated systems and networks
  - ❑ How to maintain the chain of trust throughout the OHCA?
  - ❑ Where are the vulnerabilities?
  - ❑ Is one CE or BA a back door to the entire net?
  - ❑ How allocate -
    - ❑ Liability for risk?
    - ❑ Responsibility for detecting attacks?
    - ❑ Responsibility for incident response?

# Hybrids

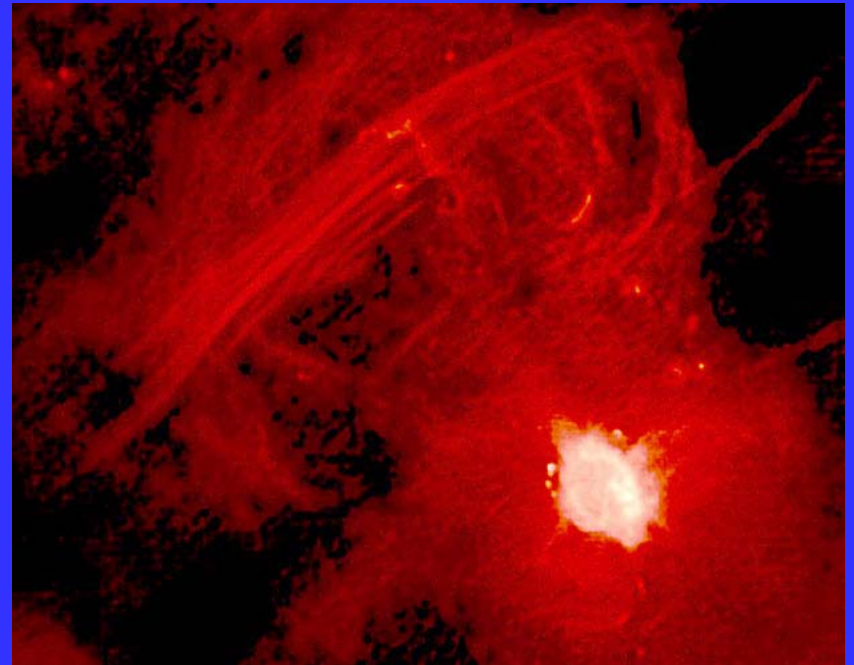
- ❑ Covered entities that have covered and non-covered functions
- ❑ Designate as a hybrid
- ❑ Designate “health care components”
- ❑ Firewall between health care components and rest of the covered entity
  - ❑ Governmental hybrids can use MOUs to pass PHI outside the firewall and within the entity
  - ❑ Not a governmental entity? Too bad! 67 Fed. Reg. 53206-07.
- ❑ Security for hybrid: follows the PHI

# Holistic HIPAA Contracting



**Privacy rule as an  
Astronomical Object**

- \* Massive!**
- \* Sucks in all attention and thought!**
- \* Nothing escapes the event horizon!**



# Holistic HIPAA Contracting

★ The privacy rule is just one of many factors!

★ Widen the focus!

★ Include security!



# Holistic HIPAA Contracting For Security

**General HIPAA Rule 1: When creating, moving, or storing PHI with a counterparty, the standard of care requires using a contract.**

*(Exception: provider-to-provider for treatment)*

**NOTE: People will object on grounds of inconvenience, and expense (eg, we haven't used written trading partner agreements in the past)**

**Response: Read the statute; security is key – maintain the chain of trust!**



# Holistic HIPAA Contracting For Security

## General HIPAA Rule 2: When drafting a contract involving PHI, use a checklist.

- ☑ Trading partner agreement – UCC Article 4A
- ☑ Consumer – EFTA and Regulation E (Federal Reserve)
- ☑ ESign and UETA
- ☑ Disclaim application of UCITA (MD & VA)
- ☑ Prudential considerations (e.g., state tort law + HIPAA statute; state contract law; state and federal consumer protection laws; criminal sentencing guidelines + business judgment rule)
- ☑ Security rules – specific requirements, prudential considerations
- ☑ TCS rules – 45 CFR § 162.915
- ☑ Privacy rule requirements

# **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**

# Information Security Plan

- Security is more than just a password-protected login
  - It MUST be implemented in layers
  - Should be as transparent as possible
    - Otherwise, people will just go around it
- An organization must be ready to protect, detect, and respond immediately to any type of adverse event – incident response is a pre-planned reaction

# Expense v. Security Achieved

