HIPAA Summit IV
Workshop II: Security
HIPAA Litigation Risk Management

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

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
- Lesson for plans?

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**

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
- Though an indirect concern of plans, we are obligated to think about providers as a potential terrorist delivery system, like airplanes and mail (plans do not want to be a back-door source into providers' systems)

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)

Case to Consider

U.S. v. Mead Corp. (U.S. Sup. Ct. No. 99-1434, June 18, 2002)

- Customs Service ruling letters about tariff clarifications
- Question: does Court treat this ruling letter as authoritative - does it have presumptive weight, like a statute or regulation, so that the Court must defer to the agency's view? ("*Chevron* deference")
- Answer: No - give Chevron deference only to
  - Notice and comment rule makings (formal proceedings)
  - Administrative adjudications
- Consequence: weight of informal agency guidance depends on how good the reasoning is (persuasive?)
- Value of HHS's informal guidance?

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.

2.
7.

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 ho Placed Orders, Sites re Left Footing the Bills

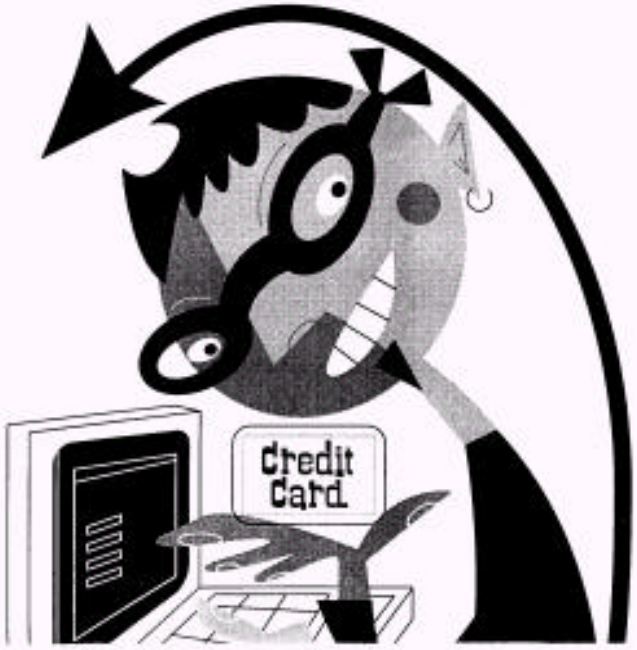
By Julia Angwin
Reporter of The Wall Street Journal

SEEMED LIKE a valid order. A cus-ner calling herself Amina Hadir vis-d Victor Stein's Web site in April and dered a $780 collector's edition of The liard Encyclopedia, which Mr. Stein re-dwired.

e the transaction was authorized by lr. Stein shipped the book to an address occo provided by the customer and t no more about it. After all, says the rk sugar broker who writes about bil-o the side, 25% of his sales come from billiard enthusiasts.

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

er mind that Visa had authorized the ard transaction or that Mr. Stein could



A Stolen Laptop Can Be Trouble If Owner Is CEO

By Nick Wingfield
Staff Reporter of The Wall Street Journal

Irwin 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 Hefferman, a security consultant with R.J. Hefferman Associates Inc. in Branford, 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

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 of the Plan

- Verisign issuance of 3 spoofed certificates for use on MSN. Question: how many others?
- Same facts at a plan:
  - Could not trust anything on the system.
  - Must you take the whole system down?
  - If so, how do you function? Dangers?
  - 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**
- ✓ **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."

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, 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)

Proposed: "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."

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)
  - state law?

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

Structured approached - 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)

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

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?
- 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?

Expense v. Security Achieved