Essentials of HIPAA Security Litigation Risk Planning

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

"HIPAA Is the Law"

- How do lawyers analyze HIPAA?
- How is that different from how normal people look at HIPAA?
- What is your institutional exposure to various kinds of legal liability?
- How should you factor legal analysis - the legal perspective - into your business decisions about HIPAA?

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?

Sources of Law

- Statutes
- Administrative Regulations
  - Implement statutes
  - Must be consistent with governing statute
  - Administrative Procedure Act - “Notice and Comment Rule Making”
- Administrative Adjudications
- Administrative Guidance
- Case Law - cumulative outcomes
  - Court cases: U.S. District Court > U.S. Court of Appeals > U.S. Supreme Court

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?

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

What Are the Guideposts?

- The statute controls the regulations
  - Look out for regulations that may not fit the statute
  - Interpret regulations in light of the statute
- Factor in other sources of law (*e.g.*, from criminal and civil litigation) that apply
- Establish a framework of legal reasoning, and expect some lack of reality
- Be practical (is there a choice)?
  - Business decisions guided by legal analysis and a refined common sense

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**
- ✓ **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**

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.

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, and particularly providers, must contemplate security threat and response models, and their human, business, and legal consequences
- You are obligated to think about providers as a potential terrorist delivery system, like airplanes and mail

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)

Example: 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?

Administrative Requirements and Risk Management

Various administrative requirements (*Privacy and Security*)

- **Document all complaints received (process protection)**
- **Apply sanctions to members of workforce who fail to comply (how stringent?) (suits by workforce members who believe they have been denied fair process; suits by patients who think their complaints were swept under the rug)**
- **Mitigate any harmful effects of violations to extent practicable (extent of this obligation?)**
- **Implement appropriate policies and procedures (process protection that also looks at outcomes)**
  - **"Reasonably designed. . .to ensure compliance," taking into account covered entity's**
    - **Size**
    - **Type of activities**
    - **Note: "This standard is not to be construed to permit or excuse an action that violates any other. . . requirement. . ."**

Technical Security Mechanisms (Data in Transit)

- ✓ For each organization that uses communications or networks
- ✓ Protect communications containing health information that are transmitted electronically over open networks, so that they cannot be easily intercepted and interpreted
- ✓ Over open networks, some form or encryption required
  - ✓ integrity controls
  - ✓ message authentication
- ✓ Network controls
  - ** abnormal condition alarm
  - ** audit trail to facilitate a security audit
  - ** *irrefutable* entity authentication
  - ** event reporting for operational irregularities (self-reporting)
- ✓ Why limit encryption to open networks if your greatest threat is internal?

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

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

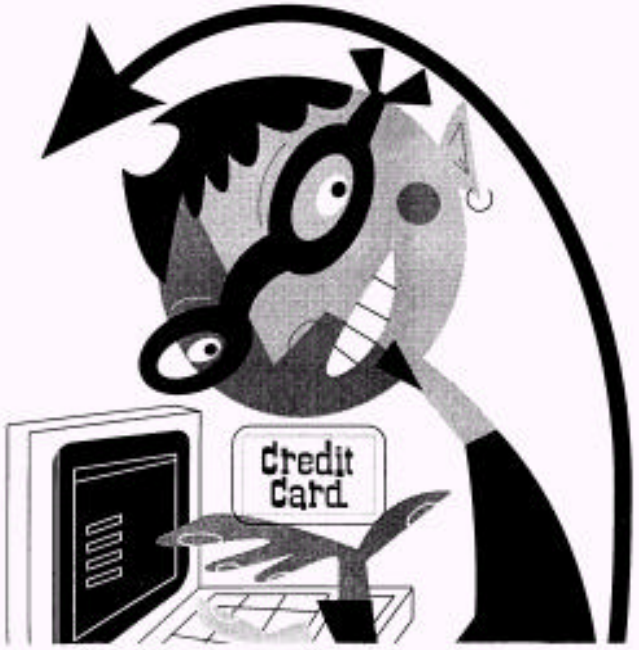
By Julia Angwin
Reporter of The Wall Street Journal

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-dered.

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-sank 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 it 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 lap-top chock full of business secrets gets ripped off?

Mr. Jacobs, the chief executive and founder of **Qualcomm** Inc., had his laptop stolen from a jour-nalism 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 in-formation 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 pow-erful tools: new portable technologies like laptop computers, hand-held electronic organizers and cellular phones. While the devices offer unprece-dented flexibility to executives, they also lead to frightening lapses in information security be-cause of the sheer volume of data than can be hauled around on them.

Basically, business data have moved from pa-per to digits, but many companies aren't moving as quickly to update their security measures. Lap-top 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-

HIPAA Compliance Requires Asymmetric Encryption

- No other practical way to meet the privacy and security requirements
- HHS is fully aware the encryption will be necessary
- HHS may not be aware that
  - "Covered entities" typically interconnect (cobble together?) disparate systems from a variety of vendors; these are inelegant solutions ("kluges")
  - "Covered entities" can't buy an end-to-end computer system solution
  - Adding an encryption layer (with all attendant business process changes) will be difficult, time-consuming, expensive - and impossible for some legacy systems

Public Key Infrastructure (PKI) Technology

Performs all these functions AUTOMATICALLY, but:

- **Must be engineered for the industry ("technically mature")**
  - ***E.g.*, financial industry**
- **Must be PROPERLY IMPLEMENTED (hard to do!)**

"Currently there are not technically mature techniques…[for] nonrepudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques."

Risk Management Issues in PKI System Creation

- Certification Practice Statement
  - Explains CA's digital certificate issuance and revocation policies
- Certificate Policy
  - Specifies conditions of use of a digital certificate
- Contracts allocating liability among entity, CA, users
- Insurance and limitation of liability issues
- Federal law: ESign, GLB
- State contract law (UCC, UCITA, UETA, etc.)
- Legal adequacy of threat and response models and security and privacy policies

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?

PKI in the Real World of the Hospital

- Verisign issuance of 3 spoofed certificates for use on MSN. Question: how many others?
- Same facts at a hospital:
  - Could not trust anything on the system.
  - Safety/ malpractice concern (remember systems integration issue?)
  - Must you take the whole system down?
  - If so, how do you function? Dangers?
- What's the systems answer in managing risk?
  - Constant hot backups?
  - With ongoing integrity checking and encrypted storage?
  - Where would you buy that?

Risk Management Options with Regard to PKI

- VPNs (Virtual Private Networks)
  - Not as secure as PKI, unless they incorporate PKI
  - Suffice for the moment as an acceptable practice in the industry?
  - Not all VPN's are equal
- SSL (Secure Socket Layer)
  - Current prevailing standard?
  - Known vulnerabilities!
  - Litigation trap.
- Not much else. . . .

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: HIPAA v. malpractice
- How do you pay to administer all this?

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

Biometrics

THE WALL STREET JOURNAL TUESDAY, MAY 2, 2000 B5

Microsoft to Use 'Biometric' Tools To Bolster Security for Windows

By Jathon Sapsford
Staff Reporter of The Wall Street Journal

Microsoft Corp. has agreed to include in future versions of its Windows operating system a type of software that uses "biometric" devices such as fingerprint or eye scanners to boost online security.

Microsoft today will announce it signed a licensing agreement with closely held **I/O Software** Inc. of Riverside, Calif., which has a proven "application programming interface," or API, for biometrics technology. This essentially is a program that lets fingerprint or eye scanners communicate with operating systems.

Some see these scanners, which identify users based on unique individual characteristics, as eventually enhancing or replacing computer passwords. A crucial step in this process, say those in the industry, is the acceptance by both producers and users of an API that allows easy employment of the devices. The goal is to create a software infrastructure that would let users simply plug in biometric devices and start using them to log on.

Microsoft's move, which comes as the company is battling antitrust enforcers, may surprise some participants in a consortium of technology companies that have been working on a separate API. Yet that consensus-based effort has been slow, and many within the consortium privately said they welcome news of I/O's deal as something that will speed the development of a broader market for biometric devices.

The vision behind the development of the appliances encompasses both the business and consumer markets. In the case of fingerprint scanners, for example, users would place their thumb on a silicon wafer to identify themselves rather than—or in addition to—punch in a password or credit-card number. The device can ensure greater protection for those who use computers for everything from financial transactions to data mining.

Microsoft warned, however, that it will take time for all this to develop. Officials at the Redmond, Wash., software company wouldn't say exactly when this new software will be available on Windows. Corporate customers, whose acceptance is crucial to the development of a market for such devices, also warn that beyond a common API, other obstacles exist, including the need for large infrastructure investments to support biometric devices.

Several customers, meanwhile, are running their own tests of this technology, which has been used for decades by police, government agencies and the military. Microsoft's deal "validates" the use of biometrics technology as a security option, said Matthew Martin, vice president of security architecture at **Chase Manhattan** Corp. The huge New York bank is running an internal pilot program in which staff log on to computers using fingerprint scanners instead of passwords.

Biometric software *in future versions of Windows will allow users to employ new security tools such as Sony's fingerprint recognition device.*

AMERICA ONLINE INC.

Pact With Homestore.com Is Set for Stock and Cash

America Online Inc., Dulles, Va., said it has reached a five-year pact to promote **Homestore.com** Inc., a residential real-estate Web site, on AOL's online properties. Under the terms of their agreement, Homestore, of Thousand Oaks, Calif., will give AOL $20 million in cash and 3.9 million Homestore shares, or about 5% of the company's common stock outstanding. Based on Friday's closing share price of $18.25, that stake was worth $71.2 million. Homestore is required to meet undisclosed stock performance targets throughout the length of its deal with AOL. Homestore rose $4.625, or 25%, to $22.875 in 4 p.m. trading on the Nasdaq Stock Market. AOL fell 31.25 cents to $59.625 in 4 p.m. composite trading on the New York Stock Exchange.

MCI WORLDCOM INC.

Bernard J. Ebbers, chief executive officer of **MCI WorldCom** Inc., Clinton, Miss., received $935,000 in salary and a $7.5 million bonus in 1999, according to the company's annual proxy statement. Mr. Ebbers also received option grants last year for 1.8 million shares with a potential value of $52.73 million, assuming a 5% annual rate of return, or $133.6 million assuming a 10% rate of return. Mr. Ebbers's salary was unchanged from 1998, though the CEO is slated to receive a raise to $1 million annually in 2000. That will match the salary William T. Esrey, Sprint's chief executive, is slated to receive as chairman of the combined company, which will be called WorldCom.

Firewalls and Intrusion/ Anomalous Event Detection

- Internal Network (location of intrusion/ anomalous event detection + logging)
- Firewall
  - Proxy firewall
- Internet (source of threats)
- Detection is useless without the ability to analyze attack and respond very fast ("real time") and effectively
  - E.g., outsourced monitoring service

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?**

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)
- Security is the framework for privacy

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

Initial Steps in Implementing HIPAA Security

How do you know where you need to get, *i.e.*, the level of security you need?

- **Fundamentally a legal question, with these elements:**
  - **HIPAA statute**
  - **Regulations: all the elements of security**
  - **State of art in the [defense/ financial] industry**
    - **Encryption - PKI**
    - **Access/ authentication controls - biometrics**
    - **Process controls (including logs/ audit)**
    - **Total systems implementation**
    - **Constant surveillance**
    - **Prevention, detection, response, in all processes, not just in technology**
- **You need this analysis to guide the consultants!**
- **Leads to business risk decisions**

Litigation & Operational Perspective

Litigation is likely, so use these criteria:

- **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?**
- **Certification (*all systems* carrying PHI and their interoperation)**
  - **Accreditation**
  - **White paper -- wedi.org >>SNIP**

A Litigator's View of "Best" Practices

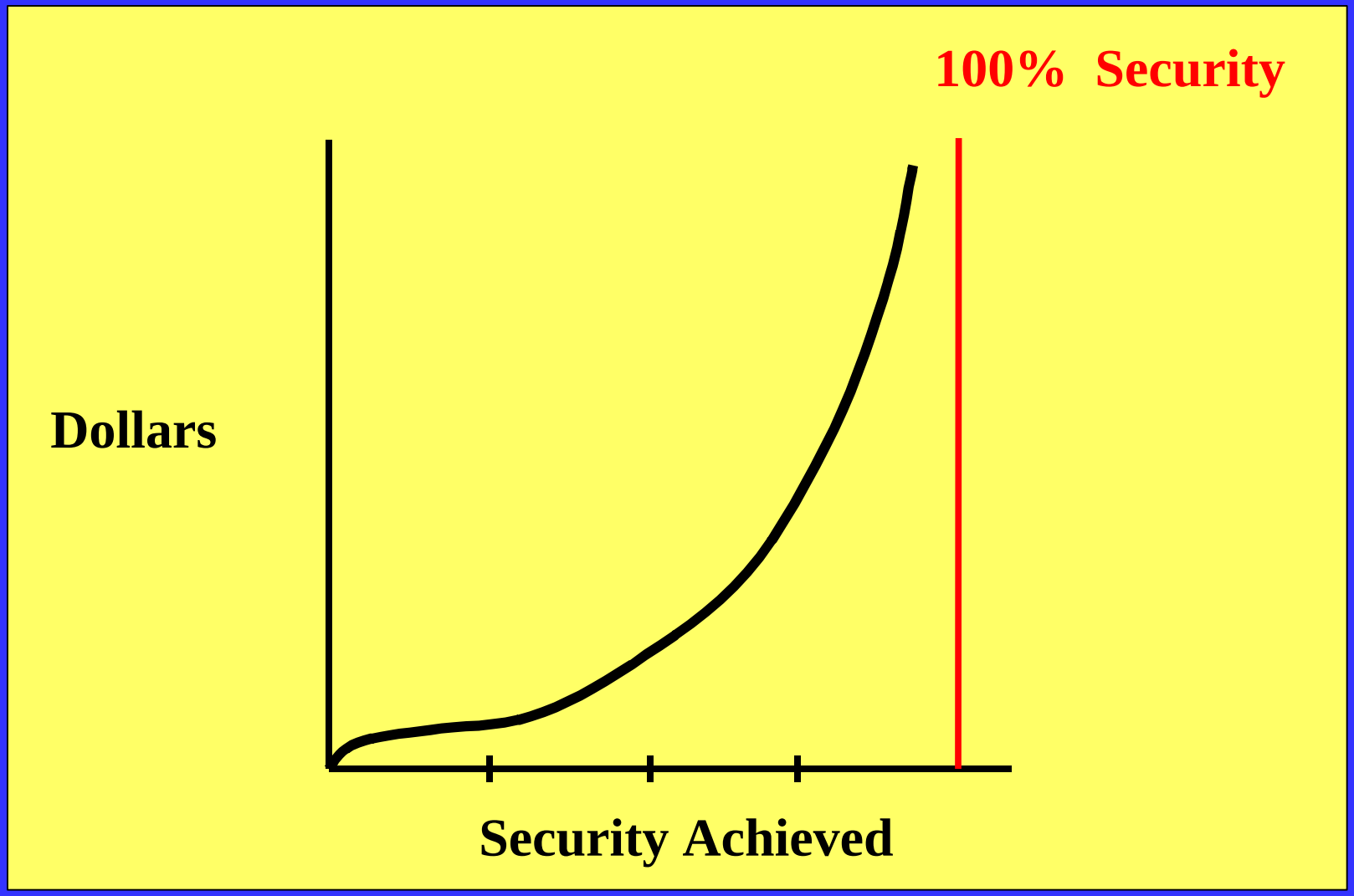
- In security field, "best practices" are at NSA, CIA, etc.
- In commercial security field, "best" practices are at banks and other financial institutions, or in defense industry
- Health care prevailing industry practices
  - Not "best"
  - Superseded by HIPAA statute and regs
- Consider "appropriate" or "recommended" practices
- Don't make your expert vulnerable

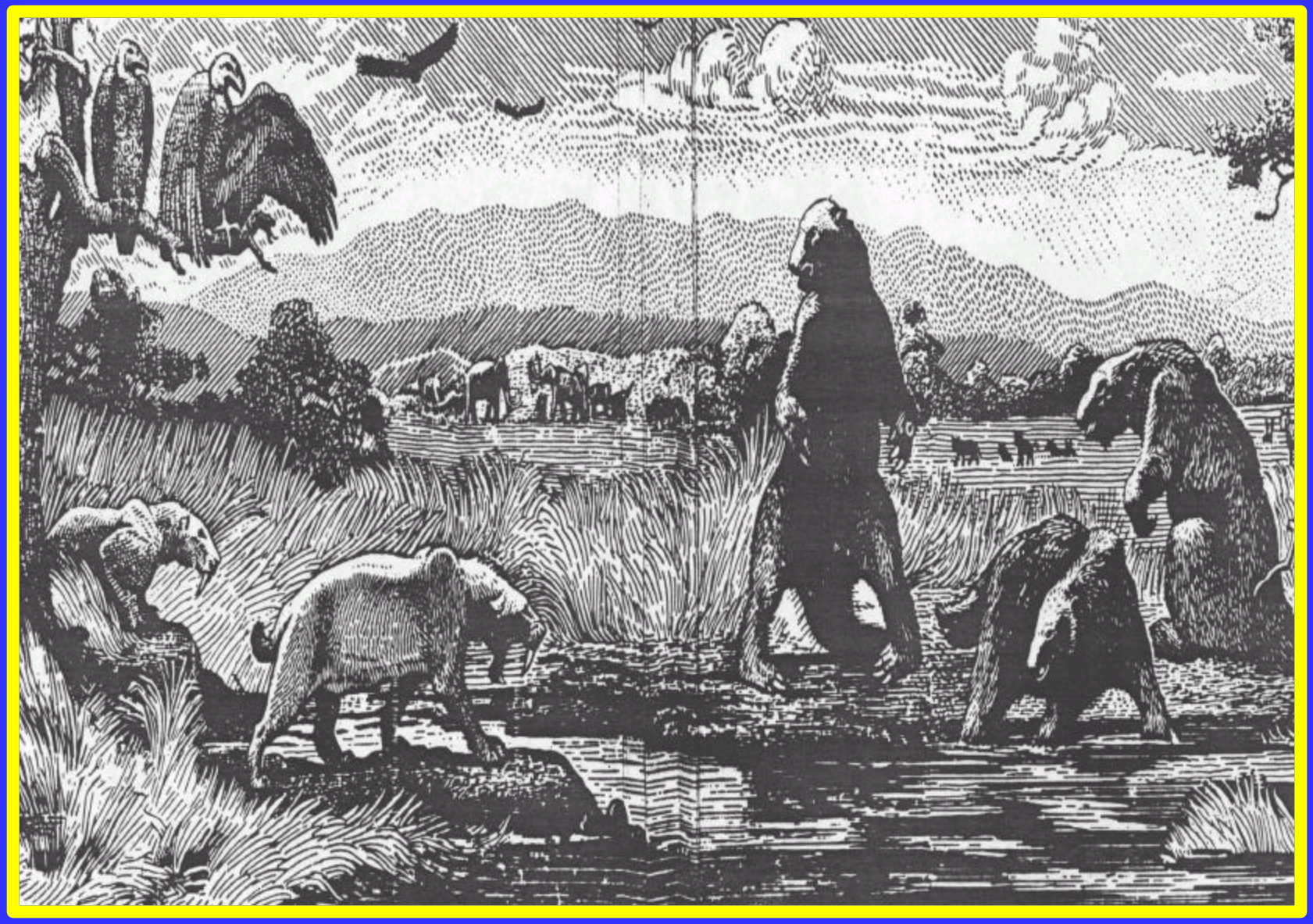
Expense v. Security Achieved

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.