An Introduction to HIPAA Security and Privacy: Context and Analysis

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

The Health Insurance Portability and Accountability Act of 1996

- HIPAA amends the Social Security Act
- Initial impact: portability of health insurance
- Responds to concerns about the privacy of electronically stored and transmitted health records
- Responds to rapid technological advances and opportunity to reduce healthcare transaction costs using EDI
- Congressional humor: “Administrative Simplification”

HIPAA's Components

- **National Provider Identifier (Final Rule - June, 2000)**
- **National Employer Identifier**
- **9 Transaction & Code Sets (Final Rule - August, 2000)**
- **Privacy Standards (December 22, 2000 - 637 pages in Federal Register)**
- **Security Standards (Proposed August 1998 - 49 pages in Federal Register - final rules expected in March-April-May?)**
- **Missing: National Patient Identifier**

HIPAA's 9 Transaction Sets

- First report of injury (delayed)
- Eligibility for a health plan
- Healthcare claim attachment (delayed)
- Healthcare claim status
- Referral certification and authorization
- Premium payments
- Enrollment or disenrollment in a health plan
- Claim payment & remittance advice
- Healthcare claim or encounter

HIPAA Final Privacy Rules

Federal Register, December 28, 2000

- "Effective" February 26, 2001
- Enforced starting February 26, 2003

Very long and very complicated

- Rules plus commentary: 367 pages
- Rules alone: 31 pages

How are the rules organized?

- For each topic: a general rule
- Many exceptions (flexibility - attempts to capture current practice)

HIPAA Security and Privacy

Best way to master the rules?

- Place in context - understand relationships
  - Security Rules to Privacy Rules
  - Enforcement
- Use principal definitions as anchors
- Understand rules' philosophy
- Identify basic mechanisms that implement this philosophy
- Realize that the devil is in the details (*i.e.*, the exceptions are very important)

An epidemic of complexity!

Privacy Rules - Background

1. **In 1996, in HIPAA, Congress gave itself 42 months to pass medical records privacy legislation**
2. **Otherwise, HHS would adopt final regulations in 6 months**
3. **Congress missed its deadline**
4. **HHS proposed privacy regulations in November 3, 1999**
5. **50,000 + comments filed**
6. **February 21, 2000 deadline for HHS final privacy regulations - missed**
7. **HHS released final privacy regulations on December 22, 2000 (published 6 days later in Federal Register)**

HIPAA Context

The Fear

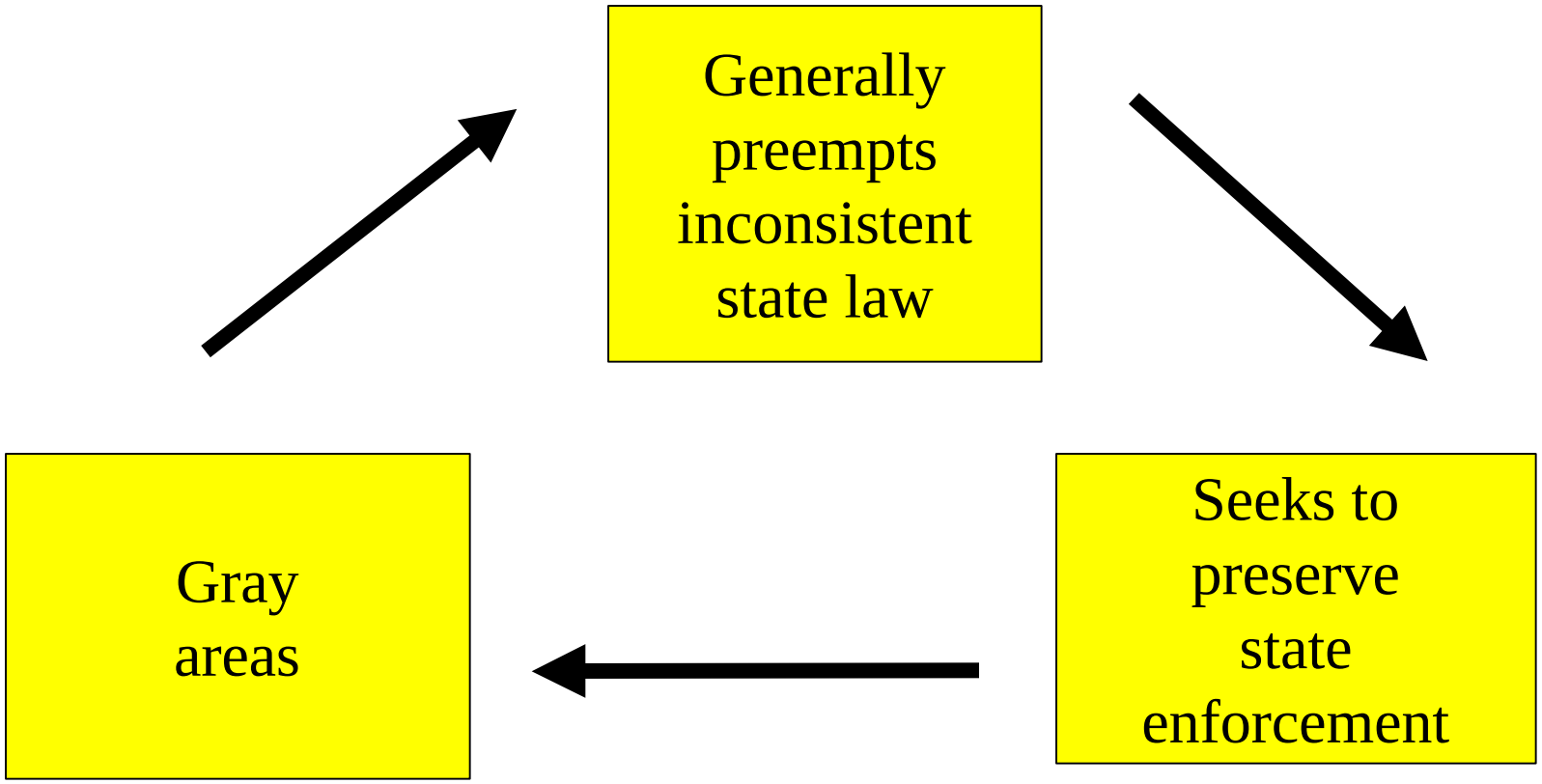
Once patients' records are stored electronically on networks, a couple of clicks can transmit those records all over the world!

Subsidiary Motivations

Loss of personal control over personal information

Anger at constant barrage of marketing messages

HIPAA's Relationship to State Law



HIPAA Security and Privacy Rules

- Jurisdiction (§160.102):
  - Provider (or agent for provider), health plan or clearinghouse (a "covered entity") who:
    - Transmits health information in electronic form
    - "In connection with" a "standard transaction"
- Once there is jurisdiction -
  - The HIPAA rules apply: Security, Privacy, Transaction Sets, etc.
- Definition of "protected health information" (§164.501)
  - ***Oral*** or recorded, maintained, or transmitted in any form or medium
  - Created or received by provider, payor, clearinghouse (a "covered entity")
  - Relating to an ***identified*** individual's past, present, or future
    - Physical or mental health or condition, or
    - Provision of health care, or
    - Payment for provision of health care (past, present, future)

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."

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 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.**

  NSA sets the rules

  At its best, the security is awesome

  Then there's John Deutsch and Wen Ho Lee

  (and many others)

Other Potential Civil Liability - Ratcheting Duty of Care

Tort - Invasion of Privacy

Publication of Private Facts

False Light (akin to defamation)

Unauthorized commercial use

Tort - Defamation

Tort- Fraud

Statutory - Consumer Fraud

Contract - Breach of confidentiality clauses/policies

Qui Tam (whistleblower) suits

HIPAA Security Standards

HHS's Security Standards must

- be comprehensive
- address all aspects of security in a concerted fashion
- be technology-neutral (technology changes quickly)
- be scaleable
- Security rules' "need to know" principle meshes with privacy rules' "minimum necessary disclosure" principle

Standards - A Matrix

- **Administrative Procedures**
- **Physical Safeguards**
- **Technical Security Services (data Storage)**
- **Technical Security Mechanisms (data transmission)**

Administrative Procedures

- **Certification (“as part of, and in support of, the accreditation process”)**
- **Chain-of-trust partner agreement (now called a business associate agreement under both the security and the privacy rules)**
- **Contingency plan**
- **Formal mechanism for processing records**
- **Information access control**
- **Internal audit**

Administrative Procedures

Internal audit. To enable the organization to identify potential security violations, an ongoing internal audit process would be required, i.e., an in-house review of the records of system activity including logins, file accesses, and security incidents, maintained by an entity.

Administrative Procedures

- **Personnel security**
- **Security configuration management**
- **Security incident procedures**
- **Security management process**
- **Termination procedures**
- **Training**

Administrative Procedures

Personnel security. To prevent unnecessary or inadvertent access to secure information, all personnel with access to health information must be authorized to access health information after receiving appropriate clearances. This Administrative Procedure has six (6) required implementation features.

Administrative Procedures

Security incident procedures. To ensure that security violations are reported and handled promptly, organizations would be required to implement accurate and current security incident procedures. This Administrative Procedure has two (2) required implementation features.

****5th Amendment self-incrimination?**

Administrative Procedures

Security management process. To ensure the prevention, detection, containment, and correction of security breaches, a process for security management would be required. The process would be required to include the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets (both physical and electronic), and to include four (4) implementation features.

****5th Amendment self-incrimination?**

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

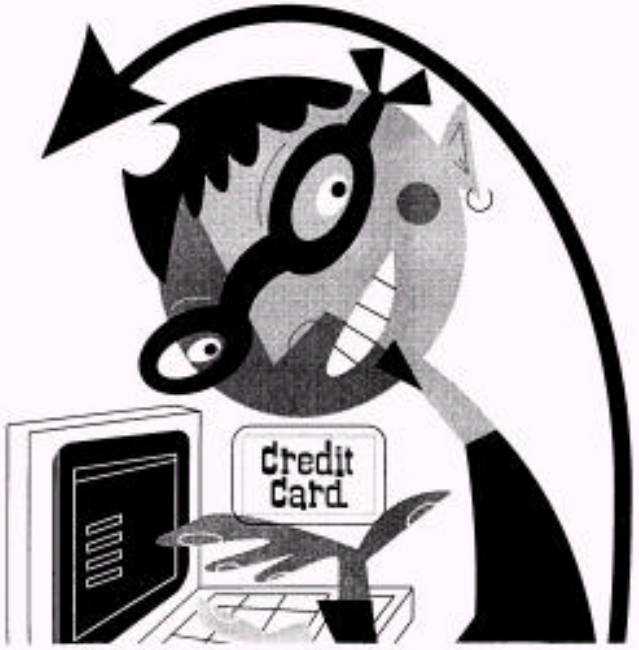
By Julia Angwin
Reporter of The Wall Street Journal

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-dwered.

e the transaction was authorized by Ir. 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 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 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-

Physical Security

- **Assigned Security Responsibility**
- **Media Controls (formal, documented policies)**
- **Physical Access Controls**
- **Policy on Workstation Use**
- **Secure Workstation Location**
- **Security Awareness Training**

Technical Security Services (Data at Rest)

- **Access Control**
  - **Documented procedures for emergency access**
  - **Text-, role-, or user-based access**
  - **Encryption optional**
- **Audit Controls**
- **Authorization Controls**
- **Data Authentication**
  - **Auto logoff**
  - **Unique user identifier for tracking**
  - **Biometric, password, or other personal identifier**

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)**

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**

  **** "Covered entities" can't buy an end-to-end solution**

  **** Adding an encryption layer (with all attendant business process changes) will be difficult, time-consuming, and expensive**

Public Key Infrastructure (PKI) Technology

Performs all these functions AUTOMATICALLY

- **Must be engineered for the industry ("technically mature")**
- **E.g., financial industry**

At the moment, it's not engineered for health care

Ask system vendors - be alert for vaporware

Not much else….

"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."

Adding PKI Encryption to Medical Systems

- **“Kluged” systems are tough enough to operate without encryption**
- **Some legacy systems cannot be adapted to encryption**
- **PKI engineering challenge: volume & speed**

  **** Experience: adding PKI = molasses**
- **No standard = no interoperability (a huge, very real, impediment)**
- **Expense is high (e.g., $10-$15 per digital certificate)**

Caveats

- **Encryption can't do the job alone**
  - **Systems approach to implementation**
- **Experience teaches that computer technology projects are difficult to implement well**
- **Most organizations are not used to living with HIPAA's level of security (e.g., constant access control, entity authentication, and surveillance)**
- **There's a significant litigation potential and substantial criminal jeopardy to individuals even with PKI**

Access is a Separate Set of 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 (eventual answer)

- **How do you pay to administer all this?**

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

HIPAA Emergency Access

- **“Glass-break”**
- **What’s the Procedure?**

  Civil and criminal liability?

  HIPAA

  Tort (state law - med mal)

HIPAA Final Privacy Rule - Context

Good news: by and large, an improvement

- **Implementing the Privacy Rule is doable**

Relationship of Privacy to Security

- **Security is the framework**
- **Privacy is implemented within that framework**
- **Implementing some aspects of Privacy must await release of the Final Security Rule**
  - **A couple of months (March - May?)**
  - **But we know enough about the Security Rule so that there is no reason to wait, and every reason to start**

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

HIPAA Context

Enforcement - 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 the end game?**
  - **Certification (*all systems* carrying PHI and their interoperation)**
  - **Accreditation**

HIPAA Final Privacy Rule

- **De-identified health information - an option**
  - **Effect - remove info from ambit of the Privacy Rule**
- **Privacy rule (§164.514) tells you**
  - **What de-identified health information is:**
    - **Does not identify an individual and**
    - **No reasonable basis to believe could use to identify individual (alone or in combination with other information)**
  - **How to create it!**
- **To de-identify PHI:**
  - **Prescribed checklist and methodology - remove:**
    - **Names; SSNs; med. Record, account, license, vehicle, etc. nos.,**
    - **Geocodes (zip codes unless <20,000)**
    - **URLs, email, telephone & fax numbers, other unique IDs**
    - **Biometric identifiers, full face photos & comparable images, etc.**
  - **Use a qualified statistician who determines "risk is very small"**
    - **Scientific methodology**
    - **Document methods and results**

HIPAA Final Privacy Rule

Philosophy: Patient-Consumer:

- Is entitled to notice
  - Major exception is an emergency
- Must expect that, within a medical care facility, PHI will be shared to facilitate care, payment, business operations
- Is entitled to expect that caregivers will be careful about how PHI is used and disclosed
- Has a right of access to PHI
- Has a right to protest mistakes in PHI and have PHI corrected or otherwise amended
- Is entitled to control the use of PHI in certain circumstances:
  - Research
  - Fund raising
  - Marketing
- Should know that the government can get PHI for law enforcement and health care oversight

HIPAA NOTICE

Basics

- **Explains the organization's privacy policies**
- **Complex rules for when and how (email, mail, alternative addresses) notice is given**
- **A covered entity may reserve the right to change its privacy policy (§164.520(b)(1)(v)(C))**
  - **Must be explicit in the notice**
  - **Must explain how changes will be communicated**
  - **If not: a change can operate only prospectively**
    - **Straightjacket - keeping track of different regimes is costly and impractical**
  - ***Therefore, in the notice, invariably reserve right to change the policy***

HIPAA NOTICE

Required Elements

- **No specified format, but -**
- **Plain language**
  - **organized to serve needs of reader**
  - **short sections**
  - **clear and concise descriptions**
  - **short sentences**
  - **active voice**
  - **use of “you” and other pronouns**
- **Other than English (Title VI, 1964 Civil Rights Act)?**
- **Standard header**

HIPAA NOTICE
STANDARD HEADER

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

HIPAA NOTICE

- **Contents (§164.520(b))**
  - **All uses and disclosures of patient's PHI that - *without authorization* - covered entity (plan or provider) is**
    - **Permitted to make and**
    - **Required to make**
  - **Covered entity's (provider's or plan's) policies with respect to these uses and disclosures**
- **Categories of uses and disclosures for notice purposes**

HIPAA NOTICE

- **Description, including at least one example, of covered entity's use and disclosure**
- **Detailed description of *each other* purpose for which entity is *permitted* or *required* to use or disclose without patient's consent or authorization**
- **Any more stringent state law limits on use or disclosure**
- **Statement that other uses and disclosures will not be made without the individual's written authorization**
  - **And that individual may revoke the authorization**
- **Separate statement if entity intends to engage in:**
  - **Appointment reminders**
  - **Communications about treatment alternatives or other health-related benefits**
  - **Fund raising for the covered entity**
  - **A health plan's disclosing PHI to the plan sponsor**

HIPAA NOTICE

Brief description of how the individual may exercise any of these rights:

- **To request restrictions on use of disclosure of PHI for treatment, payment, health care operations (and that the entity need not agree)**
- **To receive confidential communication of PHI**
- **To inspect and copy patient's own PHI**
- **To amend patient's own PHI**
- **To receive an accounting of disclosures of PHI other than for treatment, payment, and health care operations**
- **To obtain a paper copy of the notice**
- **To complain to the entity and to the Secretary of HHS**
  - **Brief description of how**
  - **Statement that there will be no retaliation**
- **Contact (name or title, telephone number)**

Web site? Then notice must be displayed prominently.

HIPAA Definitions - Kinds of PHI

- **Consent required (§164.506)**
- **Authorization required (§164.508)**
- **No consent or authorization required, but patient *must* have chance to agree or object (§164.510)**
- **No consent or authorization required, and patient *need not* have chance to agree or object (§164.512)**

HIPAA Concepts

(from context of rules, not specific definitions)

Consent

- More general
- Relatively less rigorous protection for patient's PHI
- Covers
  - Treatment
  - Payment
  - Health Care Operations
- Relates to notice requirements

Authorization

- More specific
- Relatively more rigorous protection for patient's PHI
- Usually not for
  - Treatment
  - Payment
  - Health Care Operations
- Covers optional items
  - Research
  - Marketing/ fundraising
- Relates to notice requirements

Kinds of PHI - Consent Required

§164.506 - for treatment, payment, health care operations

Exceptions for 2 types of providers:

- Indirect treatment relationship (*i.e.*, consultative, lab, radiology services)
  - Indirect treatment provider may in some cases elect to seek consent
  - But then it is bound by patient's refusal (think before you ask!)
- Treatment of inmates of a correctional institution

Exceptions for 3 types of treatment situations (must document the elements):

- Emergencies (attempt to obtain as soon as practicable later)
- Required by law to treat and consent is refused
- Substantial barriers to communication - consent clearly inferred from circumstances using professional judgment

If no consent -

- Provider may refuse to treat (unless law mandates treatment - exception then applies as described above)
- Health plan may refuse to enroll (during enrollment process only)

Kinds of PHI - Consent Required

§164.506 - for **treatment, payment, health care operations**

If consent revoked in writing, which a patient has a right to do, then, upon receipt of the revocation:

- Provider must stop using and disclosing PHI, ***except to the extent that the covered entity has taken action in reliance on the consent*** (what does this mean?)
- Provider may refuse to continue to treat
- Health plan may disenroll the individual (assuming the consent was sought in conjunction with the individual's enrollment)
- Ethical and malpractice problems?

If conflict with an authorization or other written permission:

- Covered entity must follow the most restrictive document
- May ask patient for new consent or communicate with patient
- If oral communication, covered entity must
  - Document the patient's preference
  - Act in accordance with the preference

Kinds of PHI - Consent Required

- **§164.506 - Combination rules**
- **Consent may not be combined in a single document with the covered entity's notice of privacy practices (which we covered earlier)**
- **Consent may be combined with other types of written legal permission other than an authorization (*e.g.*, informed consent, consent to assignment of benefits, narrow consent under state law to share HIV/AIDS information) if:**
  - **Each is *visually* and *organizationally* separate**
  - **Each is separately signed and dated**
- **Consent may be combined with an authorization when**
  - **Research includes treatment**
  - **Some of patient's treatment is research-related and some is not**

Kinds of PHI - Consent Required

(§164.506 (f))

Joint consents for organized health care arrangements

- **Clinical or operational integration among legally separate covered entities**
- **Various listed arrangements (*e.g.*, hospital, group health plan) - key is patient's expectation of integration and joint management**
  - **Advertising - holding out to public of the joint operation**
- **If develop a joint notice, than can use a joint consent**
- **Effect - patient consents to use and disclosure of PHI by each covered entity for treatment, payment, health care operations**
- **The consent must identify the covered entities with "reasonable specificity"**
- **If a joint consent is revoked, the covered entity that receives it must inform the other affected entities "as soon as practicable"**

Content of Consent

- Plain language
- Refer patient to the covered entity's notice; state that the individual has the right to review the notice before signing the consent
- A statement that the covered entity has reserved the right to change its privacy practices
  - How the entity's notice may change
  - How the patient can get revised notices
- Statement that the patient may ask for restrictions on how PHI is used or disclosed
  - Covered entity need not agree to the restrictions
  - If the covered entity agrees, then the restrictions are binding
- Statement that the patient may revoke consent in writing, except to extent that the entity has relied on the consent
- Signed and dated by the patient

Kinds of PHI - Authorization Required

(§164.508)

Use an authorization for

- All uses and disclosures of PHI that are
- Not otherwise permitted or required under the Privacy Rule

Psychotherapy notes

- Exception to general rule that treatment is covered by a consent
- A provider needs an authorization to use or disclose psychotherapy notes for treatment except for use
  - By the originator of the notes for treatment
  - In training programs (individual, joint, group, family counseling)
  - To defend a legal action or proceeding brought by the patient
  - Required for oversight of the originator
- Cannot combine an authorization for use or disclosure of psychotherapy notes with any other authorization

Kinds of PHI - Authorization Required

(§164.508)

Other authorizations can be combined <u>except when</u> the covered entity conditions treatment, payment, enrollment, or other benefits on one of the authorizations

Authorizations with conditions ok for:

- **Research-related treatment**
- **Health plan enrollment or eligibility for benefits (determinations, underwriting, risk rating)**
- **Payment**

Kinds of PHI - Authorization Required

Authorizations - form and content requirements

- **Core elements**
  - **Specific, meaningful description of PHI**
  - **Names or specific identification of persons (or classes of persons) who will use or disclose PHI**
  - **Expiration date or event**
  - **Statement that individual may revoke**
  - **Warning that PHI's redisclosure may be unprotected**
  - **Signature of individual and date**
- **Reasons for invalidity**
  - **Expiration date or event has passed**
  - **Not completely filled out - missing element**
  - **Entity knows revoked in fact**
  - **Entity knows material information is false**
  - **Improper compound authorization**

Kinds of PHI - Authorization Required

Authorizations - additional form and content requirements when for covered entity's own use or disclosure

- **Statement that covered entity will not condition treatment, payment, enrollment in health plan, or eligibility of benefits on receiving the authorization**
- **Description of each purpose of the use or disclosure**
- **Statement that patient may inspect and copy the PHI**
- **Statement that patient may refuse to sign the authorization**
- **If use or disclosure will result in direct or indirect remuneration to the covered entity from a third party, a statement to that effect**

Kinds of PHI - No Consent or Authorization Required, but Patient ***Must*** Have Chance to Agree or Object

(§164.510) Uses are

- Directory information
  - Name, location in facility, condition in general terms (no specific medical information); religious affiliation
  - Disclose to people who ask for the patient by name, and to clergy
- To next-of-kin or another person involved in the patient's care
- Covered entity must inform patient of right to object and to restrict information (when practicable or as early as practicable)

- Different rules if individual is present or not, or lacks capacity, or in emergency circumstances
  - Professional judgment, experience, common practice
  - Disclosure to family, other relatives, close personal friends, personal representative
- Disaster relief - use and disclosure to public or private agency authorized by law or charter to assist in relief efforts

Kinds of PHI - No Consent or Authorization Required, and Patient *Need Not* Have Chance to Agree or Object

- **"National priority" uses and disclosures - complex rules**
  - **Public health**
  - **Reporting of abuse, neglect, domestic violence**
  - **Health oversight activities**
  - **Judicial and administrative proceedings**
  - **Law enforcement**
  - **Decedents; cadaveric donation**
  - **Serious threats to health or safety**
  - **National security; protective services**
- **Covered entity has discretion to disclose for these purposes**
  - **However, nothing in rule allows covered entity to refuse or restrict a disclosure mandated by law**

Minimum Necessary Rule

- (§164.514) **Presumption: not generally applicable in treatment settings.** Otherwise, a covered entity must limit requests for PHI to the minimum necessary
- Routine and recurring disclosures of PHI
  - Covered entity must develop policies and procedures (may be standard protocols)
  - To limit PHI to the minimum amount reasonably necessary to achieve purpose of the disclosure
- All other requests for disclosures of PHI
  - Covered entity must develop criteria & review individually
  - Same requirement for policies, procedures, protocols
  - To limit PHI to the minimum amount reasonably necessary to achieve purpose of the disclosure
  - Applies to request from workforce professional or business associate who represents that request is for minimum necessary PHI
  - Request for entire medical record requires ***specific justification***

Marketing and Fundraising

(§164.514 (e))

Definition: Communication ("to make a communication") about a product or service, a purpose of which is to encourage purchase or use.

Covered entity does not need authorization to use PHI for marketing when it observes these procedures

- **Face-to-face encounter:**
- **Products or services of nominal value; or**
- **Concerns health-related products and services of the covered entity or a third party, and**
  - **Allows patient to opt out of future communications; and**
  - **Entity determines that the communication may be beneficial to health of type or class targeted**
- **Communication includes required elements, such as statement regarding direct or indirect remuneration**

Marketing and Fundraising

(§164.514 (f))

Covered entity, without authorization, may use or disclose to business associate or institutionally related foundation certain PHI for fund raising for its own benefit

- **Demographic information relating to an individual**
- **Dates of care provided to an individual**
- **Must include information on how individual can opt out and "make reasonable efforts to ensure" that opt-outs are effective**

Business Associate Agreements

Business Associate (§160.103) - A person or entity who, on behalf of a covered entity, and not as a member of the entity's workforce, performs or assists in the performance of a function or activity involving individually identifiable health information (includes, *e.g.*, data analysis, quality assurance, utilization review, claims processing), or legal, accounting, actuarial, consulting, data aggregation, management, administrative, accreditation, or financial services.

Business Associate Agreements

Useful definitions and concepts

- **Workforce: employees, volunteers, trainees, other persons (including in many cases independent contractors)**
- **A covered entity may be a business associate of another covered entity.**
- **Trading partner agreement - an agreement relating to the exchange of information in electronic transactions (EDI). Can be a BAA.**

Business Associate Agreements

Useful definitions and concepts (continued)

- Hybrid entity: a covered entity that is a single legal entity and whose covered functions are not its primary functions (must protect PHI in covered functions).
- Common control: the power, direct or indirect, significantly to influence or direct another entity's actions or policies.
- Common ownership: an ownership or equity interest of 5% or more.
  - **Note: <u>legally separate covered entities may designate themselves as a single affiliated covered entity if all are under common ownership or control</u>**

Business Associate Agreements

BAA between covered entity and BA must:

- **Establish permitted uses and disclosures**
  - **Can't go beyond what the covered entity can do with PHI**
  - **Can authorize use and disclosure for the proper management and administration of the BA**
  - **Can authorize data aggregation services (combining with data from *another* covered entity)**

Business Associate Agreements

BAA between covered entity and BA must require that the BA:

- **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**

Business Associate Agreements

BAA between covered entity and BA must require that the BA:

- **"Ensure" its agents (including subcontractors) agree to same restrictions as in the BAA**
- **Make PHI available to patients who request it**
- **Make PHI available to patients to amend and incorporate changes**
- **Make available an accounting of PHI disclosures**
- **Make available to HHS its internal practices and books relating to use and disclosure of PHI**
- **Destroy PHI upon BAA's termination**

Business Associate Agreements

- The covered entity must enforce the BAA (§164.504(e)):
- Covered entity is not in compliance if:
  - knew of
  - pattern or practice (what about a single violation?) of
  - material breach or violation (difference ?)
  - UNLESS
    - Covered entity takes reasonable steps to
      - cure breach or
      - end violation or
    - If those steps are unsuccessful
      - terminates the BAA, or
      - if termination is infeasible, reports problem to HHS

Business Associate Agreements

Consider impact of other laws

- Gramm-Leach-Bliley (financial privacy)
  - Implementing federal regulations - 7 agencies
  - Implementing state statutes and regulations
    - NAIC model regulation
- ESign
- UCC Article 4A (EDI)
- UETA
- UCITA
- EU Privacy Directive and U.S. Safe Harbor

Accessing and Amending PHI

(§164.524)

- **Patient has a right of access except for**
  - **Psychotherapy notes**
  - **Material compiled in anticipation of litigation**
- **Time limit: generally 30 days, can be extended to 60 under defined circumstances**
- **Entity can deny access request for**
  - **Excepted categories**
  - **PHI of inmate, where there is danger**
  - **Certain research situations where patient agreed to the denial in the consent**
  - **Entity obtained the PHI from a confidential source**

Accessing and Amending PHI

(§164.524)

Entity can deny access request by individual or personal representative, subject to review as follows:

- Reasonable likelihood of danger to
  - Life or physical safety of
  - The patient or another person
  - As determined by licensed health professional using
  - Professional judgment
- PHI makes reference to another person and
  - Reasonably likely to cause substantial harm to that other person
  - As determined by licensed health professional using
  - Professional judgment
- Patient may request review by entity's review official (who did not participate in the original denial decision)
  - Transaction costs? Legal duties of care?

Accessing and Amending PHI

(§164.526)

Individual has right to have covered entity amend PHI in the designated record set

- **Covered entity can deny amendment if**
  - **It was not originator of the PHI and there is reasonable basis to believe that the originator is not longer available to act**
  - **PHI is not part of the designated record set**
  - **PHI would not be available for inspection under Privacy Rule**
  - **PHI is accurate and complete**
- **Covered entity can require patient to request amendment in writing and specify reason**
- **Covered entity must agree or refuse within specified time limit, and inform the patient of decision and reason**

Accessing and Amending PHI

(§164.526)

Individual has right to disagree with covered entity's decision to refuse to amend PHI in the designated record set

- Patient may demand that covered entity include patient's request for amendment and entity's denial in any future disclosure of the PHI
- Covered entity must permit patient to submit statement of disagreement
  - Covered entity may reasonably limit length of statement
  - Covered entity may prepare rebuttal and furnish copy to patient
  - Covered entity must document all this in designated record set
  - Covered entity must include all this in future disclosure of PHI, if patient so requests
- Transaction costs? Policy and business process choices?

Administrative Requirements

(§164.528)

Patient has right to accounting of covered entity's disclosures of PHI for last 6 years (some exceptions, *e.g.*, national security, law enforcement)

(§164.530)

Various administrative requirements

- **Designate privacy official and contact person or office**
- **Training for each member of covered entity's workforce**
  - **Initial**
  - **Whenever a material change**
- **Appropriate administrative, technical, physical safeguards (security rule)**

Administrative Requirements

Various administrative requirements (continued)

- Document all complaints received
- Apply sanctions to members of workforce who fail to comply (how stringent?)
- Mitigate any harmful effects of violations to extent practicable (extent of this obligations?)
- Refrain from intimidating or retaliatory acts
- Implement appropriate policies and procedures
  - "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. . . ."

Privacy in the Security Context

The Privacy Rule must be integrated into security procedures that are

- Comprehensive and effective
- Address all aspects of privacy and security in a concerted fashion
- Log or otherwise retain the audit trail information so that it can be
  - Retrieved quickly and inexpensively
  - When feasible, screened to trigger a notice or alarm in time to prevent a mistake or intrusion
  - Reviewed on a regular schedule (at least daily) to identity and correct mistakes not caught earlier

Medical Record Privacy - Politics

Impetus: mainly e-commerce abuses

Congressional Privacy Caucus (Sens. Bryan & Shelby, Reps. Barton & Markey)

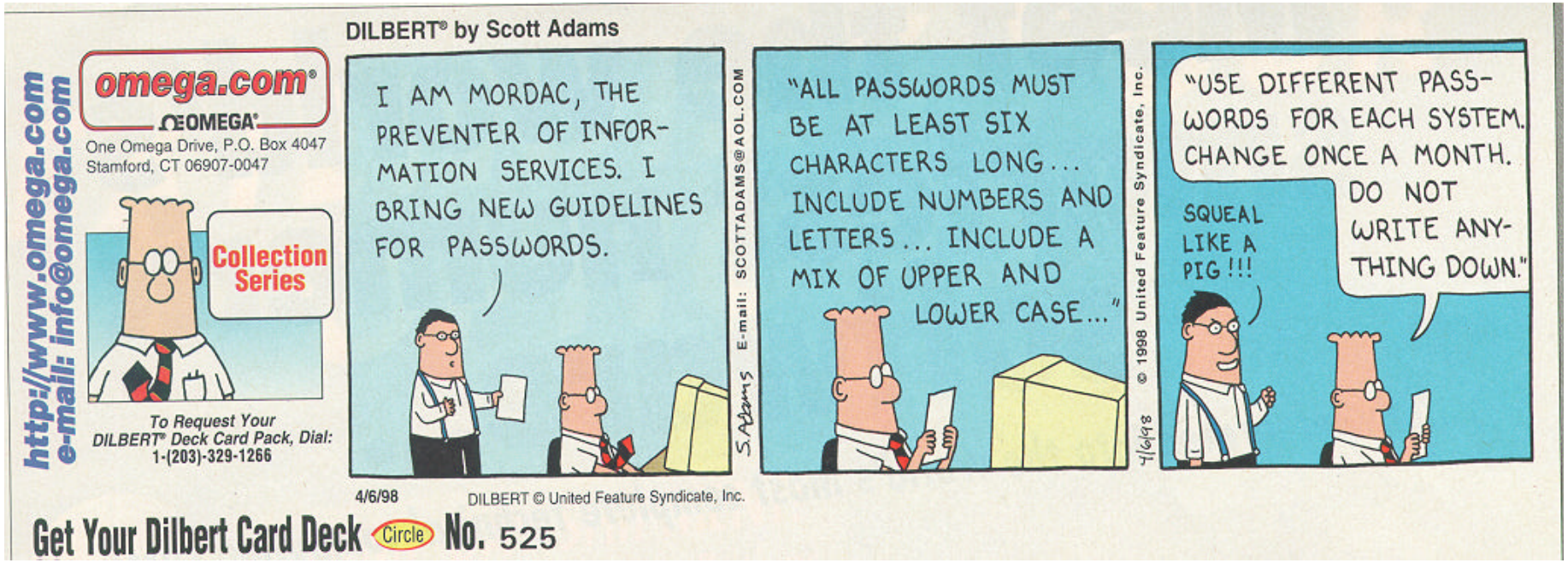
4 Principles:

- **Notice**
- **Access & correction**
- **Consent**
- **Non-preemption (federal floor)**

Initial Steps in Implementing HIPAA Security

- **Initial analysis of gap between enterprise's**
  - **Present level of security**
  - **Where you need to get**
- **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: the security matrix**
    - **State of art in the [defense/ financial] industry**
      - **Encryption - PKI**
      - **Access controls - biometrics**
      - **Process controls**
      - **Constant surveillance**

Implementing What HIPAA Requires



Personnel Security

THE WASHINGTON POST

900,000 People Awaiting Pentagon Security Clearances

Backlog Blamed on Computer Woes, High Turnover, Increased Requirements

By WALTER PINCUS
Washington Post Staff Writer

More than 900,000 people are awaiting Pentagon security clearances while the unit responsible for conducting background investigations struggles with a huge backlog and computer problems, according to a report by the Defense Department's inspector general.

The Defense Security Service has started, but not completed, background checks on about 400,000 of those people, who include military personnel, civilian Pentagon employees and workers at private firms with defense contracts requiring security clearances.

In addition, the DSS has not even begun checking on 505,000 civilian and military personnel who were cleared for classified information years ago and are due for periodic reinvestigation, said the agency's director, retired Lt. Gen. Charles J. Cunningham Jr.

As of February, it took an average of 306 days to investigate a new employee for a top-secret clearance and 300 days to reinvestigate a person who has held a top-secret clearance for five years, the study found.

In the five months that ended in

ries.

In his recent Senate testimony, Mancuso attributed the backlog to a high turnover in Pentagon personnel, new requirements for reinvestigations and an increase in the level of security clearances required of new Navy and Air Force recruits.

"We have a continuing problem of large numbers of personnel in mission-critical or high-risk positions without updated security clearanc-

> "We have a continuing problem of large numbers of personnel . . . without updated security clearances."
>
> — **Donald Mancuso**
> Deputy inspector general

es," Mancuso said. He added that

Biometrics

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.

HIPAA Security - Mandatory Choices

Functions to be secured

+ **Access**

  Physical & personnel security (e.g., nurses' stations, ICUs)

  passwords +?

  biometrics?

+ **Transmission**

  PKI

+ **Storage**

PKI? (Of course)

HIPAA Security - Mandatory Choices

- **All clinical systems**
- **External and internal email (remember, the greatest threat is internal)**
- **Any communications systems carrying PHI (at any time)**

  External email/Internet

  Physician consults

  Communications with patients

  Communications with payors

  Communications with regulatory authorities

Enterprise Compliance Plan for Information Security

Achieving a reasonable level of security is a multifaceted task

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

Note: investment compared to the level of security achieved is not a linear relationship!

Enterprise Compliance Plan

- **Not simply an IT project**
- **Not only a compliance project**
- **Requires a team with leadership from the highest level of the enterprise, because**

  [1] the cultural and business process changes will have a pervasive impact,

  [2] they will cost a great deal, and

  [3] they carry the very real potential for an adverse impact on the delivery of care and on research

Will the national security model interfere with delivery of health care?

- **Sheer cost**

  **** The cost-benefit analysis is highly politicized**

  **** E.g., the congressional privacy caucus; pending legislative proposals**

  **** An unfunded mandate**

- **Business process change in the clinical setting - regime of surveillance and jeopardy**

- **Worries about impact on patient care, research, teaching, and the ethic of medicine**

- **Seeking legislative relief is inevitable**

For the Moment

- **Continue “gap analysis” on a more comprehensive scale**
- **Inventory present practices (e.g., Internet consults)**
- **All IS, clinical, business system purchases**

  **** HIPAA design considerations**

  **** HIPAA contract language regarding future compliance (time frame), termination rights, change management (security - required item)**

Criminal Law - Federal Sentencing/Prosecution Guidelines

Structured approached - covers organizations

Why here? Because HIPAA violations can be criminal.

Some definitions from Sentencing Guidelines:

- **“High-level personnel of the organization”**
- **“Substantial authority personnel”**
- **“Condoned”**
- **“Effective program to prevent and detect violations of law”**
- **“Willfully ignorant of the offense”**

“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)

Federal Sentencing Guidelines

Note the top-down risk

Next Steps

- **Preserve attorney-client, work product privileges**
- **Make policy elections (*e.g.*, single covered entity?)**
- **Begin drafting security and privacy policies (legal as well as operational documents)**
- **Contemplate training**
- **Consider impact of other laws (GLB, UCC 4A, ESign, UETA, UCITA, EU Safe Harbor)**
- **Factor into E-commerce plans**
- **Include in vendor negotiations and all procurements**
- **Assess budget impact**

Selected Privacy Questions Awaiting the Final Security Rule

- **How much detail, and about what, will be required for audit trails?**
- **What are the requirements for certification and accreditation of privacy and security policies and practices?**
- **How much self-reporting of violations will be required, and to whom?**
- **Now that PHI includes oral communications, will we have to encrypt voice channels (*i.e.*, telephone systems), or will there be an exception for telephone communications in the Security Rule?**