

# **WEDI/ SNIP: Selected HIPAA Implementation, Policy, and Political Issues**

**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](mailto:richardmarks@dwt.com)**

Copyright 2001 Richard D. Marks

All Rights Reserved



**When will there be a  
HIPAA security  
rule?**

# 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.”

(42 USC §1320d-2(d)(2); in effect now - does not require final security or privacy rules to become effective)

# **Final Privacy Rule, §164.530(c)(1), Administrative Requirements**

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

**On April 14, this security rule will also be in effect!**

# Administrative Requirements

- ◆ 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. . . .”**

# 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 future state?
  - ◆ Certification (*all systems* carrying PHI and their interoperation)
  - ◆ Accreditation

**How do we begin?**

**What are some of the  
business issues?**

**How do they relate to  
HIPAA politics?**

# Ten Beginning Steps

1. Preserve attorney-client, work product privileges
2. Envision the *future state*!
3. Make policy elections (*e.g.*, single covered entity, organized health care arrangement, hybrid organization, Bus. Assoc. Contracts?)
4. Initial security analyses
5. Begin clinical and business process redesign; draft security and privacy policies (legal as well as operational documents)

# Ten Beginning Steps

6. **Audit trail design (realism for purposes of review; real-time alarms; quick, affordable retrieval)**
7. **Contemplate training needs**
8. **Consider impact of other laws (GLB, UCC 4A, ESign, UETA, UCITA, EU Safe Harbor, state law preemption) (for the lawyers)**
9. **Include in vendor negotiations and all procurements**
10. **Assess budget impact**

# **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!**

# HIPAA Initial Business Decisions

How can the enterprise operate to enable *joint notices* and *joint consents* that will simplify operations?

- ✓ Single provider - single Covered Entity
- ✓ Multiple providers - single Covered Entity  
(“control” test):

Legally separate covered entities may designate themselves as a single affiliated covered entity if all are under common ownership (5% or more equity) or control (significant influence)

- ✓ Multiple providers - Organized Health Care Arrangement

Clinical or operational integration among legally separate covered entities - key is patient’s expectation of integration and joint management - holding out to public of the joint operation

If develop a *joint notice*, then can use a *joint consent*

- ✓ Hybrid organization
- ✓ Business associate agreement

# HIPAA Initial Business Decisions

## Disease management and patient advisory issues

☞ **What is the role of the entity, *e.g.*, and Pharmacy Benefits Management company (PBM)?**

☞ **“Treatment”**

☞ **“Marketing”**

☞ **The ability of the provider and the PBM to offer care options to patients will depend in part on writing sensible policies that carefully categorize appropriate disease management services as “treatment”**

# 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**

# 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 clearances."

"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

# 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?**

# Physical Security

- **Assigned Security Responsibility**
- **Media Controls (formal, documented policies)**
- **Physical Access Controls**
- **Policy on Workstation Use**
- **Secure Workstation Location**
- **Security Awareness Training**
  
- ★ **Issue: nurses' stations as secure areas.  
(What about semi-private rooms?)**

# 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 solution
  - \*\* Adding an encryption layer (with all attendant business process changes) will be difficult, time-consuming, expensive, and impossible for some

# Public Key Infrastructure (PKI) Technology

**Must be engineered for the industry (“technically mature”)**

- Engineering for financial industry has taken decades

**At the moment, it’s not engineered for health care**

- 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)

**Ask system vendors - be alert for vaporware (“HIPAA compliant”)**

**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.”**

# 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)
  - *Auto logoff*
  - *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,



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

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.

### 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 WORLD COM INC.

Bernard J. Ebbers, chief executive officer of MCI WorldCom Inc., Clinton, Miss., received \$95,000 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 \$133.8 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 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
- ✓ Long list of patient's rights (*e.g.*, right to amend PHI)
- ✓ 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
- ✓ And much more mind-numbing detail!
- ✓ *Does it make sense to hand a new patient a consent form that looks, hefts, and reads like an SEC-approved prospectus?  
What's the benefit?*

# Selected 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?

# **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 (timing)**

# Medical Record Privacy - Politics

## HHS Secretary Thompson - Feb. 28, 2001:

- ◆ Final privacy rules will be reopened for comment for 30 days.
  - ◆ Deadline: 5 pm EST, March 30, 2001
- ◆ Effect on existing final privacy rules:
  - ◆ Will become final April 14, 2001.
  - ◆ Congressional Review Act of 1996 - to change final rule, Congress must act within 60 days (by April 14). President lacks inherent power to change rules.
- ◆ Administrative Procedure Act issues - New notice and comment period *after* Privacy Rules are final?
- ◆ Industry lobbying effectiveness with new Administration?
- ◆ Congressional reaction? Pressure on Administration?

# Medical Record Privacy - Politics

**National Governors' Association - Feb. 27, 2001:**

**“Since enactment of HIPAA in 1996, it has become clear that the length and structure of its implementation period is unrealistic and untenable. The statute directs the U.S. Department of Health and Human Services to develop a series of regulations, each with their own implementation deadline. Unfortunately, it will be impossible for states to effectively comply with any part of HIPAA until all relevant regulations have been finalized and their implications can be assessed as a whole. Therefore, the Governors call upon Congress to amend HIPAA to revise the implementation schedule among the following principles:**

# Medical Record Privacy - Politics

National Governors' Association - Feb. 27, 2001:

- \* No state or other covered entity should be required to begin implementation of HIPAA until such a time as all HIPAA regulations have been finalized.
- \* A single, uniform date of compliance should be established after the finalization of all HIPAA regulations. Congress must allow states a sufficient and reasonable time period in which to implement this complex law and its multitude of regulations.”

# Medical Record Privacy - Politics

## HHS Electronic Advisory Group Favors Federal Preemption of State Privacy Rules

A Department of Health and Human Services electronic data advisory group says it favors the preemption of state privacy standards by the federal rules.

During a Feb. 26 and 27 meeting, the Workgroup for Electronic Data Interchange voted to support the principle that the privacy rules mandated by the 1996 Health Insurance Portability and Accountability Act should become the standard for all states.

WEDI members discussed several highly debated issues in the rule, but decided that the only substantive action they would take would be to recommend that Congress support full preemption.

WEDI also may ask state legislators to hold off on enacting new state privacy laws during the two-year implementation period of the final federal rule.

# Medical Record Privacy - Politics

- ✓ **Congressional Privacy Caucus**
  - ✓ **Chairs: Sens. Shelby (R-AL) & Bryan (D-NV), Reps. Markey (D-MA) & Barton (R-TX)**
- ✓ **Impetus:**
  - ✓ **E-commerce marketing abuses**
  - ✓ **Consistent surveys: consumer fears of medical record abuse on the Internet**
  - ✓ **Consistent, effective lobbying by privacy advocates**
- ✓ **4 Principles**
  - ✓ **Notice**
  - ✓ **Access & correction**
  - ✓ **Consent**
  - ✓ **Federal floor - no preemption of stricter state laws**

# Medical Record Privacy - Politics

## Lobbying approach to comment period

- ✓ Congress is as important as the Administration
- ✓ Health care industry should acknowledge weaknesses of relying solely on umbrella organizations
  - ✓ Benefits of grassroots comments
- ✓ Health care industry must acknowledge lack of operational experience with new rules
  - ✓ Beware of “sky is falling” effect
  - ✓ Choose targets in rules carefully
- ✓ Health care industry must have a new approach to first principles (privacy = motherhood)

# Medical Record Privacy - Politics

What might first principles be?

Recognition of *patient's* important competing rights:

1. Right to be free of unnecessary burdens (ineffectual mandates) when seeking care (*e.g.*, sample notice as akin to SEC-mandated prospectus)
2. Right to receive care in an environment where important clinical information flows are not impeded (disproportionate restrictions)
3. Right to a proportionate government response in balance between protecting patient information and facilitating the availability of clinical information
4. Right to be free from much higher costs that will result from unnecessary record keeping

# Medical Record Privacy - Politics

## Lobbying approach - additional considerations

- ✓ The privacy rules can't be considered outside the framework of the security rules!
- ✓ The technology necessary for meeting many of the security requirements isn't available, and won't be for years:
  - ✓ PKI is not yet engineered for information systems and clinical/ business processes in the health industry
  - ✓ PKI will be difficult (often impossible) to graft onto many providers' legacy systems

# Medical Record Privacy - Politics

## Lobbying approach - additional considerations (cont.)

- ✓ *Patients* have a right to a care environment that is friendly and hospitable:
  - ✓ Constant surveillance - a necessary concomitant of the present proposed security and final privacy rules - will make hospitals and physician offices *inhospitable* settings for patients and their families (as well as for the clinicians and other staff)

# Medical Record Privacy - Politics

The privacy of patients' medical records is exceptionally important, so the approach to protecting privacy must be practical and affordable. Our process must balance consumers' easy access to health care with their privacy interests; and we should strive keep doctors' offices and hospitals as friendly places, not make them into fortresses.