goulston&storrs

think*results*

HIPAA Privacy Regulations

Enforcement, Penalties and Risk Management

HIPAA Privacy Regulations

Alan M. Reisch

James T. Hargrove


Present


Absent

What We Won't Talk About

- Detailed discussion of penalties
  - Covered by others in many sessions
  - Not certain that regulations will remain as currently established
- Detailed discussion of the current regulations
  - You need to read them, and understand them

goulston&storrs
thinkresults

This Has Happened Before - and We've Lived Through It

- Asbestosis Exposures
- Environmental Exposures
- Lead Paint Exposures
- Others Still Developing
  - Mold
  - Tobacco

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- What is Risk?
  - Exposure to something that is uncertain - that may cause you harm
- Risk Acceptance vs. Risk Aversion
  - Businesses, just like people, can either accept risk comfortably, or be risk averse
- At some point, though, Risk must be managed

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- What is Risk Management
  - What is the Risk?
  - Who is Affected by the Risk?
  - How do you Manage the Risk?

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- In many ways, there's nothing new
  - Breach of Confidentiality Always Led to Exposure
  - Tension between information needed to diagnose, treat and manage v. protection of privacy
  - Most associated risk should already be managed

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- BUT - the issue is now crystalized
- HIPAA is:
  - An objective manifestation of a perceived societal good
  - A state of mind
  - A paradigm shift
  - The essence of a standard against which you will be judged

goulston&storrs
thinkresults

What is the Risk?

- Unauthorized Disclosure of Protected Health Information

Civil Penalties
Criminal Penalties
Litigation by Individuals
Litigation by Other Providers

goulston&storrs
thinkresults

How Bad Can It Be?

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet.
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store.
- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS.
- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut.

goulston&storrs
thinkresults

How Bad Can It Be?

- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees.

- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased.

goulston&storrs
thinkresults

How Bad Can It Be?

- A speculator bid $4,000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients.
- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women.
- A few weeks after an Orlando, Florida, woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol.

goulston&storrs
thinkresults

How Bad Can It Be?

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended.
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt.
- A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression.

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Who is Impacted?
  - Multiple Covered Function Entities
    - Health Plans, HMO's
  - Health Care Clearinghouses
    - Data Processors, Billing Services
  - Health Care Providers
    - Any Person or Entity that Furnishes, Bills, or is Paid for Health Care Services

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Who is Impacted?
  - Business Associates
    - an entity that performs or assists in the performance of services for a covered entity that involves the disclosure of Protected Health Information - claims processing, administration, data analysis, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Who is Impacted?
  - Solution Vendors
    - All the Exhibitors who want to help you comply with HIPAA
  - If you assume the burden for a price you also assume the risk of loss
    - Secure e-mail providers, data scrubbers, etc.

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Managing the Risk
  - Threshold Protocols and Assessment
  - Regulatory Exemptions
    - Make it go away
  - Insurance
    - Transfer the Risk for a Price
  - Contract
    - Transfer the Risk by Agreement
  - Retention
    - Reserve for the Risk

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Threshold Protocols
  - administrative procedures
  - physical safeguards
  - technical protections relating to data storage
  - technical protections relating to access to and transmission of data

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Administrative Procedures
  - training programs, specific assignment of security responsibility, development and implementation of formal protocols for access control and data processing, protocols for reporting, responding to, and sanctioning breaches of security, procedures (such as changing locks and passwords) in the event of personnel terminations, and internal audits

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

Physical Safeguards

- physical access controls, such as identification verification procedures for physical access to data sites, clearance hierarchies based on a “need-to-know” basis, and restrictions on access to and the physical manipulation of hardware components

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Technical Protections - Data Storage
  - authentication and access control (using such methods as automatic log-off, user identification and other access controls such as biometric identification, passwords, a callback function or token-based systems)

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Technical Protections - Access & Transmission
  - alarmed, audited, and authenticated access control to transmissions (such as dedicated lines secure from tampering) or encryption, data and message authentication and integrity controls, “chain of trust” agreements with third parties who receive protected health information from the covered entity, procedures to coordinate overall security including documentation, hardware, and software systems review and virus checking, disaster and intrusion response and recovery plans, third parties certification to evaluate compliance

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Assessment
  - Compliance with HIPAA Regulations
  - Civil Penalties
  - Criminal Penalties
  - Litigation by Individuals
  - Litigation by Other Providers

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Regulatory Exemptions
  - Carve yourself a niche that isn't regulated
  - It ain't over until it's over
    - Further hearings
    - Increased pressure from industry groups
    - Cost Concerns
    - Shifting economic background
    - Where are priorities?

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Transfer Options
  - Insurance
  - Contractual Devices
  - Self-Insurance

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Insurance
  - Liability Policies
    - CGL, exclusion buybacks, extended coverages
  - Errors & Omissions
  - Directors & Officers
  - Performance & Payment Bonds
  - Manuscript Policies
    - Relation to E-Commerce

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Contract
  - Indemnification by Third Parties
    - Carefully drafted agreements
    - Party with the greater bargaining power will most often prevail in shifting risk to party with less bargaining power (as to that party's remedy, see Insurance)

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Retention
  - Save up for the eventual payment
  - Assess Exposure
    - Based on own actual errors
    - Based on perceived errors
    - Other factors
  - Protect whatever assets can be protected

goulston&storrs
thinkresults

Enforcement, Penalties and Risk Management

- Cost Considerations
  - Premiums
  - Contract Price
  - Reserves
  - Implementation
  - Monitoring
  - Ongoing Reassessment

goulston&storrs
thinkresults

CNN.com allpolitics.com with TIME

February 26, 2001

Bush delays sweeping medical privacy rules

WASHINGTON (Reuters) - In a victory for the health care industry, the Bush administration will at least temporarily delay sweeping new regulations proposed by former President Bill Clinton aimed at protecting the privacy of patients, officials said Monday.

But major insurers, health maintenance organizations (HMOs) and other groups have increased pressure on the new Republican administration to put the rules on hold, arguing that they would set "unworkable standards" and cost the industry billions of dollars a year to implement.

Under the rules, protections would be extended to personal medical records, whether written or not, and would guard against their unauthorized use by companies in hiring new employees.

As proposed by the Clinton administration, the regulations would also create new criminal and civil penalties to punish those who improperly use or disclose personal health information. These would include a fine of up to $50,000 and a year in prison for intentional disclosure. Disclosure with intent to sell the data would be punishable by a fine of up to $250,000 and up to 10 years in prison.

The rules would not, however, cover life insurers and worker compensation programs, putting the onus on Congress to close several loopholes in the regulations.

Business Insurance

March 1, 2001

HHS reopens comment period for privacy rules

WASHINGTON—Employers and others concerned about implementation of a controversial medical records privacy bill now have until March 30 to submit written comments to the Department of Health and Human Services.

HHS had originally issued its rules on Dec. 28, 2000, **but a paperwork error** pushed the effective date of the rule to April 14 from the original date of Feb. 26. HHS Secretary Tommy G. Thompson announced a few days ago that he would reopen the comment period, "to ensure a thorough review" of the issues involved. The notice of the extended comment period, which began Wednesday, appeared in the Feb. 28 Federal Register.

goulston&storrs

think*results*