HIPAA PRIVACY:
A Three Year Look Back

Barry S. Herrin, CHE, Esq.
Smith Moore LLP
Atlanta, Georgia

Thirteenth HIPAA Summit
September 26, 2006
Washington DC

Overview

- The Scope of the Problem
- Notorious Examples of Compliance Lapses
- Criminal Prosecutions
- Civil Cases Involving HIPAA
- What Next?

SMITH MOORE LLP
ATTORNEYS AT LAW

The Scope of the Problem

- The Government Perspective
  - Since April 2003:
    - Over 18,000 complaints have been made to OCR; 70 percent of these complaints have been closed
    - Over 300 of these complaints have been referred to DOJ for possible criminal enforcement, but only two (2) criminal cases have been prosecuted successfully.
    - 433 complaints made under the Transaction and Code Set standards; only 129 of them have been determined to meet a threshold of validity.
    - Only 74 Security Rule complaints have been made.
    - No civil monetary penalties have been assessed.

The Scope of the Problem

- The Government Perspective
  - Brailer's Pipe Dream: "Paper medical records are difficult to secure and keep private – records can be left unattended on people's desks, inadvertently placed in the trash, or transported among clinician offices via taxicabs or other couriers. Even when they are in secure facilities, it is not possible to restrict viewers only to the information they need to see to do their work. We rarely can identify when privacy of paper records has been compromised. *By comparison, electronic records have strict security measures in place to prevent misuse or unauthorized access by using audit trails, access permissions, and viewing restrictions*."
  - Ironically, HHS has once again received a grade of "F" (for 2004 and 2005) in its own information security measures, according to a report issued by the Government Reform Committee of the U.S. House of Representatives

SMITH MOORE LLP
ATTORNEYS AT LAW

The Scope of the Problem

- The Provider Perspective – August 2005 HIMSS Study
  - 78 percent of responding providers were compliant with the HIPAA Privacy Rule (meaning *22 percent still noncompliant after 2 years*); this number was basically unchanged from a similar HIMSS survey performed almost a year earlier.
  - "The numbers infer little or no progress with a core group of non-compliant entities"
  - The number of providers reporting privacy breaches occurring dropped – from 73 percent during the period between July and December 2004, to 59 percent during the period between January and June 2005
  - The "biggest 'roadblocks' to compliance were 'no public relations or brand problems anticipated with noncompliance' and 'no anticipated legal consequences for non-compliance'."

SMITH MOORE LLP
ATTORNEYS AT LAW

The Scope of the Problem

- The Patients' Perspective
  - February 2004 Harris poll
    - 80 percent believe that a comprehensive EHR is a good idea
    - 25 percent believe that such a record if available over the Internet would create privacy problems
  - February 2005 Harris poll
    - 69 percent believed that EHR would lead to unauthorized releases of their medical information
  - November 2005 Modern Healthcare survey
    - 67 percent expressed concern about privacy as a result of recent privacy breaches announced in the press
    - Over 50 percent were afraid that employers would use health information inappropriately
    - 13 percent had engaged in "privacy protective behavior"

Notorious Examples

- Privacy
  - February 2006 - Brigham & Women's Medical Center, Boston - repeatedly faxed patient medical records – 22 in all – to an investment bank over a period of months, and continued to do so after the bank notified the hospital that it was receiving records in error
  - Summer 2005 - Kaiser Permanente Colorado included the member identification number for all of its 190,000 plan members on mailing labels
  - October 2003 - Pakistani remote medical transcriptionist threatened to post records belonging to patients of the University of California at San Francisco Medical Center on the Internet unless she was paid. She was providing services pursuant to a pattern of unauthorized subcontracting and outsourcing of transcription services that had been conducted for several years

Notorious Examples

- Privacy (cont'd)
  - Late 2005 - Grand Rapids, MI – local TV station began an investigation showcasing medical information being thrown away in regular trash receptacles throughout the city at five medical practices. In February of 2006, the Michigan Department of Community Health notified those providers of the potential of the revocation of the practices' Medicaid provider agreements if the privacy breaches occurred again
  - December 2004 – UC Davis Medical Center or the UC Davis student health center - medical information of about 600 patients was posted on the Internet
  - All of these could have occurred without an EHR

Notorious Examples

- Security
  - Many non-healthcare examples
  - December 2005 - backup computer tapes containing medical records on 365,000 hospice and home health care patients were stolen from an employee's car after they were left there overnight in violation of company policy
  - June 2004 – University of Washington - an intruder broke into the computer system of the UW Medicine health system and had the capability to view and copy over 2 million patient medical records for 18 months until the security breach was detected

SMITH MOORE LLP
ATTORNEYS AT LAW

Notorious Examples

- Security (cont'd)
  - May 2006 – Portland OR - St. Anthony Hospital lost over 5,000 digital X-ray images on over 900 patients because of a technical failure of its information system
  - August 2005 - Joplin MO - St. John's Regional Medical Center had information on 27,000 patients stolen from a company that makes microfilm records for the hospital
  - May 2006 - American National Red Cross reported that a Missouri-Illinois Blood Services Region employee gained improper access to the records of over 1 million blood donors, including their Social Security numbers and dates of birth

Notorious Examples

- Security (cont'd)
  - December 2005 – U of Pittsburgh MC – non-medical patient information on over 700 patients was stolen when the laptop computer containing the information was stolen from a physician practice
  - December 2005 - backup computer tapes containing medical records on 365,000 hospice and home health care patients were stolen from an employee's car after they were left there overnight in violation of company policy
  - December 2005 – U of Washington, Seattle - two laptop computers containing data on 1,600 patients were stolen from the Travel Medicine Service

Notorious Examples

- From the AHIMA Privacy and Security Practice Council
  - Non-consensual disclosure – scheduler left a message on a patient's voicemail regarding ultrasound treatment and diagnosis of pregnancy; patient's daughter retrieved the message
  - Use of a common printer caused patient's cancer diagnosis and radiology report to be given to another patient by inattentive staff
  - Release of radiological report misfiled with patient's chart indicating patient had brain cancer; report actually belonged to another patient

SMITH MOORE LLP
ATTORNEYS AT LAW

Notorious Examples

- From the AHIMA Privacy and Security Practice Council (cont'd)
  - A hospital employee was terminated for disclosing to a nurse that a pregnant patient in the hospital was intending to place her newborn child for adoption; the nurse contacted the maternity ward and gave her attorney's information to the patient
  - A fax was sent from a computer to the wrong number; the fax contained information on a patient's ovarian cyst
  - Discharge instructions were misdirected between 2 patients; Patient 1 received discharge instructions for Patient 2, which contained mental health diagnosis and list of anti-depressant medications

SMITH MOORE LLP
ATTORNEYS AT LAW

Notorious Examples

- From the AHIMA Privacy and Security Practice Council (cont'd)
  - Employee permitted a relative to log on to the hospital's IT system using her password and assist her in entering patient charges into the system
  - A nurse discussed a positive pregnancy test with an adult patient while the patient's father was in the room, prior to inquiring whether the patient wanted the father present
  - A facility disposed of its medical records by throwing them away through the conventional garbage disposal methods; the landfill administrator subsequently called the facility to inform it that records were "flying around" the landfill

SMITH MOORE LLP
ATTORNEYS AT LAW

Notorious Examples

- From Our Own Engagements
  - Medical Staff Bylaws
  - Registration Problems
  - Pre-emption Problems
  - Employee Health Care

SMITH MOORE LLP
ATTORNEYS AT LAW

Criminal Prosecutions

- U.S. v. Gibson
  - Employee of Seattle Cancer Care Alliance used a cancer patient's personal information to obtain credit cards
  - 16 months in prison, $9,000 restitution
- U.S. v. Ramirez
  - Health care employee sold information on an FBI special agent to someone thought to be working for drug traffickers (actually another FBI agent)
  - Awaiting sentencing

SMITH MOORE LLP
ATTORNEYS AT LAW

Civil Cases Involving HIPAA

- *Law v. Zuckerman* (MD) - Defense counsel spoke with a physician concerning the plaintiff's medical records without the patient's permission. The court held that HIPAA pre-empted the Maryland civil practice statutes and prohibited any ex parte communications between defendant representatives and plaintiff's physician.
- *Northwestern Memorial Hospital v. Ashcroft* (IL) – DOJ sought records on so-called "partial birth abortions" in order to defend the Partial Birth Abortion Ban Act in a separate federal proceeding. The court held that HIPAA pre-empted state law in a federal proceeding; however, the interests of patient privacy and the lack of probative value of the information sought prevented the disclosure of the information without patient consent.

Civil Cases Involving HIPAA (cont'd)

- *South Carolina Medical Association v. Thompson* (SC) - Federal pre-emption provisions of HIPAA are not unconstitutionally vague and the HIPAA statute gave sufficient guidance to the U.S. Department of Health and Human Services to issue regulations.
- *Rigaud v. Garofalo* (PA) - A workers' compensation plaintiff alleged that a physician released information to her employer improperly, resulting in her dismissal. The court held that HIPAA does not create a private right of action.
- *Kalionski v. Evans* (DC) - In a case involving psychotherapeutic records, the federal court held that state privacy rules do not govern federal claims in federal court, whereas they might in diversity actions.

What Next?

- Recommendations from the Commission on Systemic Operability
- Recommendations from the National Committee on Vital and Health Statistics
- Correlation With Known Problems
- Sheer Speculation

SMITH MOORE LLP
ATTORNEYS AT LAW

Ending the Document Game: Connecting and Transforming Your Healthcare Through Information Technology

- Change both the federal “Stark” and anti-kickback statute to permit hospitals and insurers to purchase IT resources and give them to physicians
- Adopt a “complete set of interoperable, non-overlapping data standards that function to assure data in one part of the health system is, when authorized, available and meaningful across the complete range” of health care settings
- “Develop a uniform federal health information privacy standard for the nation, based on HIPAA and pre-empting state privacy laws, which anticipates and enables data interoperability across the nation”

SMITH MOORE LLP
ATTORNEYS AT LAW

Ending the Document Game: Connecting and Transforming Your Healthcare Through Information Technology

- Create a nationwide health information network
- “Develop a national standard for determining patient authentication and identity”
- “Authorize Federal criminal sanctions against individuals who intentionally access protected data without authorization”

SMITH MOORE LLP
ATTORNEYS AT LAW

Privacy and Confidentiality in the Nationwide Health Information Network

- The method by which personal health information is stored by health care providers should be left to the health care providers
- Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN
- Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN

Privacy and Confidentiality in the Nationwide Health Information Network

- HHS should monitor the development of opt-in/opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social, and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate
- HHS should assess the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means. Decisions about whether individuals should have this right should be based on an open, transparent, and public process

SMITH MOORE LLP
ATTORNEYS AT LAW

Privacy and Confidentiality in the Nationwide Health Information Network

- If individuals are given the right to control access to the specific content of their health records via the NHIN, the right should be limited, such as by being based on the age of the information, the nature of the condition or treatment, or the type of provider
- Role-based access should be employed as a means to limit the personal health information accessible via the NHIN and its components
- HHS should investigate the feasibility of applying contextual access criteria to EHRs and the NHIN, enabling personal information disclosed beyond the health care setting on the basis of an authorization to be limited to the information reasonably necessary to achieve the purpose of the disclosure

Privacy and Confidentiality in the Nationwide Health Information Network

- HHS should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools
- HHS should explore ways to preserve some degree of state variation in health privacy law without losing systemic interoperability and essential protections for privacy and confidentiality
- HHS should harmonize the rules governing the NHIN with the HIPAA Privacy Rule, as well as other relevant federal regulations, including those regulating substance abuse treatment records

Privacy and Confidentiality in the Nationwide Health Information Network

- HHS should develop a set of strong enforcement measures that produces high levels of compliance with the rules applicable to the NHIN on the part of custodians of personal health information, but does not impose an excessive level of complexity or cost
- HHS should ensure that policies requiring a high level of compliance are built into the architecture of the NHIN
- HHS should adopt a rule providing that continued participation in the NHIN by an organization is contingent on compliance with the NHIN's privacy, confidentiality, and security rules
- HHS should ensure that appropriate penalties be imposed for egregious privacy, confidentiality, or security violations committed by any individual or entity

Privacy and Confidentiality in the Nationwide Health Information Network

- HHS should seek to ensure through legislative, regulatory, or other means that individuals whose privacy, confidentiality, or security is breached are entitled to reasonable compensation
- NCVHS endorses strong enforcement of the HIPAA Privacy Rule with regard to business associates, and, if necessary, HHS should amend the Rule to increase the responsibility of covered entities to control the privacy, confidentiality, and security practices of business associates

SMITH MOORE LLP
ATTORNEYS AT LAW

Correlation With Known Problems

- Without a uniform federal privacy standard, interchange of information as contemplated by the HIPAA Privacy Rule will be impossible to achieve; the "crazy quilt" of state laws will pose practical and legal barriers to exchange of information for even treatment and payment purposes.
- Until people go to jail for privacy violations, or until lots of providers are fined, most covered entities will not take compliance seriously
- Physicians are unlikely to adopt significant privacy and security compliance structures until one or more third parties (the government, insurers, whoever) pays for the technology and gives it to them (The new Stark exception and AKS safe harbor will help here)
- Providers will have to deal with the reality that not everyone really does need all of the access to electronic records that they currently enjoy

Correlation With Known Problems (cont'd)

- Employers will need to become less tolerant of privacy and security breaches and impose significant punishments on the workforce
- Covered entities need to have protection from frivolous, groundless, and harassing complaints, at least with respect to the recovery of attorneys' fees or costs of investigation

SMITH MOORE LLP
ATTORNEYS AT LAW

Sheer Speculation

- HR 4157
- Other Developments

SMITH MOORE LLP
ATTORNEYS AT LAW

QUESTIONS?

SMITH MOORE LLP
ATTORNEYS AT LAW

Contact Information:

Barry S. Herrin, CHE, Esq.
Smith Moore LLP
877.404.7466 x1027
barry.herrin@smithmoorelaw.com

SMITH MOORE LLP
ATTORNEYS AT LAW