PROSKAUER ROSE LLP®

PROSKAUER® on PRIVACY

The Latest Developments in Health Privacy

W E B I N A R

November 9, 2006

Presented by:

Sara Krauss
Proskauer Rose LLP
New York, NY
212.969.3049
skrauss@proskauer.com

Overview

- Health care privacy before HIPAA
- HIPAA
  - What is it?
  - What are HIPAA-covered entities?
  - Overview of HIPAA Privacy
- HIPAA Privacy compliance for employers, as health plan sponsors
- Other HIPAA issues for employers
- HIPAA Security and EDI
- HIPAA Penalties; status of HIPAA compliance/enforcement

Health Care Privacy before HIPAA

- Health care providers
  - State statutory provisions and common law
- Health insurers
  - State statutory provisions, common law
  - Gramm Leach Bliley
- Special protections
  - HIV
  - Substance Abuse Treatment
  - Family Planning
- Common law on medical privacy and employers

Health Care Privacy before (and after) HIPAA

- Health care providers
  - Before HIPAA, regulated in all states with respect to medical privacy
  - HIPAA added many details to existing state medical privacy laws for health care providers
  - Many state medical privacy rules remain after HIPAA
  - HIPAA is floor, not a ceiling; where state medical privacy laws are stricter than HIPAA, and a provider can comply with both HIPAA and state law, state law will remain
- Health insurers
  - Some states regulated insurance privacy before HIPAA
  - Gramm Leach Bliley required all states to have health insurance privacy rules

Health Care Privacy before (and after) HIPAA

- Protections for specialized types of health information:
  - HIV information
    - Regulated on a state law
    - Generally subject to much stricter privacy protections than applicable to the rest of health information
  - Substance abuse treatment information
    - Regulated on a federal level
    - Cannot acknowledge that a person is a patient in a substance abuse treatment program
  - Family planning information
    - Regulated on a federal level, and under some state laws

Health Care Privacy in the Workplace: Common Law Approach

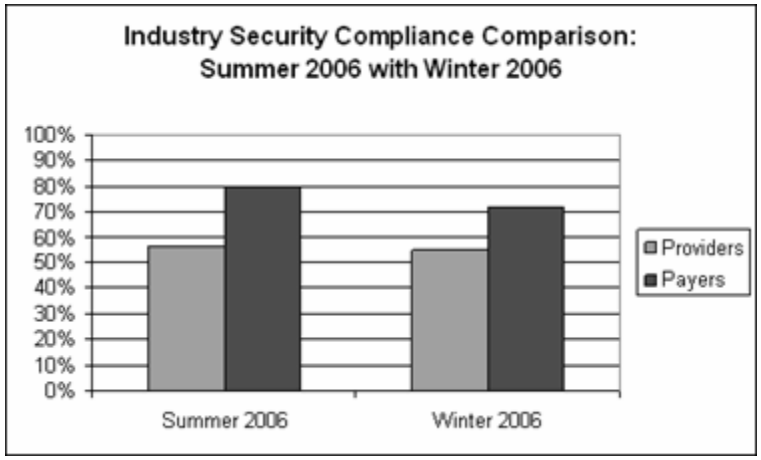
- Tort of Invasion of Privacy – disclosure claim
  - Majority View
    - Communication to a single person or to a small group of persons is NOT publicity
  - Minority View
    - Disclosure to even a small group may be publicity if the plaintiff has a special relationship with the group to whom the information is disclosed.
    - An employee has a special relationship with co-workers. *Miller v. Motorola, Inc.*, 202 Ill. App. 3d 976 (1990).

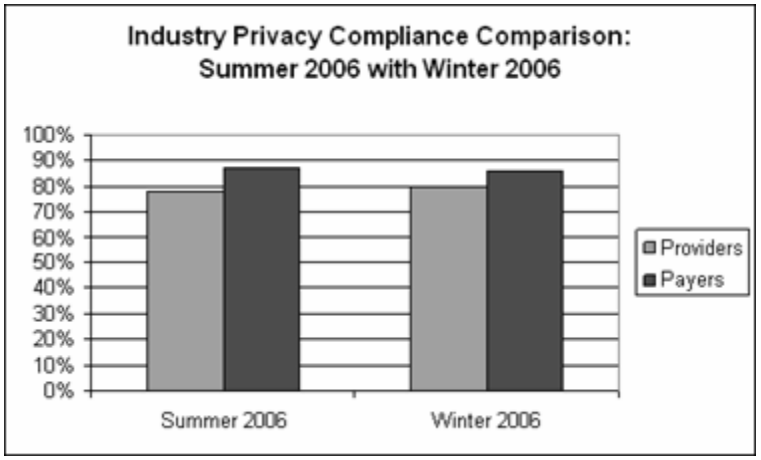
HIPAA Basics

- Just what is HIPAA anyway?
- HIPAA = Health Insurance Portability and Accountability Act of 1996[1]
- Compliance with HIPAA Privacy rules was required for most health plans and health care providers by April 14, 2003; small health plans (with annual premiums or receipts of less than $5 million) were required to comply by April 14, 2004

[1] Pub. L. No. 104-191, 100 Stat. 1936 (1996).

HIPAA Privacy and Security Compliance





Source:
http://www.hipaadvisory.com/action/surveynew/results/summer2006.htm

- Although compliance deadlines have come and gone, total industry compliance has yet to be achieved

HIPAA Administrative Simplification

- Create a framework for the standardization of electronic data interchange (EDI) in health care, including protections for the privacy and security of individually identifiable health information
- Key areas of regulations under HIPAA Administrative Simplification:
  - Privacy
  - Security
  - EDI

Covered Entities Under HIPAA

- What are covered entities under HIPAA?
  - Health plans
  - Health care clearinghouses; and
  - Health care providers who transmit any health information in electronic form in connection with one of the transactions covered by HIPAA
    - "old-fashioned" doctors who handle paper claims only or accept no health insurance technically escape applicability of HIPAA

Key Definition: Protected Health Information (PHI)

- The HIPAA Privacy Rule applies to Protected Health Information (PHI)
- PHI = individually identifiable health information that is in all forms – paper, oral, electronic
- PHI ≠ information in education records covered by the Family Educational Rights and Privacy Act (FERPA)[2]
- PHI ≠ employment records held by a covered employer in its role as an employer

[2] Pub. L. No. 93-380, 88 Stat. 484 (1974).

HIPAA Privacy Rule Compliance: Employers as Health Plan Sponsors

- Under HIPAA, like ERISA, health plan sponsors have separate legal identity from the health plans they sponsor
- HIPAA does not regulate employers in their capacity as such
- Fully insured health plans that do not receive individually identifiable information in-house have no HIPAA privacy obligations

HIPAA Privacy Compliance: Employers as Health Plan Sponsors *(cont'd)*

- Key HIPAA privacy compliance measures for employer-sponsored health plans:
  - Plan amendment
  - Privacy notice
  - Business associate agreements
  - Privacy officer
  - Policies and procedures

HIPAA Plan Amendment for Plan Sponsors

- Plan sponsors must adopt amendment to plan documents
  - Indirect regulation of employers/plan sponsors
- Plan amendment requires employer to agree that it cannot use health plan information for employment purposes or in connection with other benefits
- Plan amendment requires employer to:
  - Designate plan workforce
  - Implement a plan workforce sanctions policy
  - Establish firewall between the plan's work force (*e.g.*, Benefits Dept. personnel) and the rest of the employer's work force

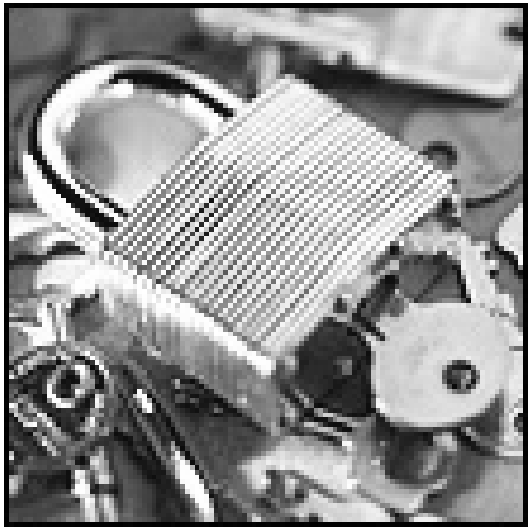
Privacy Rule Compliance: Privacy Notice

- Employer's health plans were required to distribute to all named insureds a notice of the Employer's health plans' privacy practices by April 14, 2003 (2004 for small plans), and thereafter to new participants, upon enrollment
- Reminders of the existence of the privacy notices must be sent at least once every three years

Other Implications of HIPAA for Employers

- Can we still get drug testing results or have fitness for duty exams?
- Is FMLA or ADA information protected by HIPAA?
- What about return-to-work and sick notes?
- What about employee health clinics?

HIPAA Security



- Final regulations published in February 2003
- Compliance was required by April 2005 (April 2006 for small plans)
- Substantial overlap in concept with HIPAA privacy

HIPAA Security *(cont'd)*

- Requires all HIPAA-covered entities to adopt administrative, technical, and physical safeguards to protect the security of individually identifiable health information that is maintained or transmitted **electronically**
- Adds security language for plan amendments and business associate agreements

HIPAA Civil Penalties

- In February 2006, HHS promulgated a final HIPAA Administrative Simplification enforcement rule for civil penalties[3]
- The final rule follows the fundamental HHS approach to enforcement
  - Reliance on complaints to detect violations
  - Voluntary compliance through informal approaches
  - Technical assistance

[3] 71 Fed. Reg. 8,390 (Feb. 16, 2006).

HIPAA Penalties

- HIPAA violators are subject to civil penalties
- Egregious privacy violations may be punished by criminal sanctions
- Failure to comply with HIPAA's requirements and standards will subject an entity to a civil fine of up to $100 per violation, up to a maximum of $25,000 per year for all violations of an identical requirement

HIPAA Criminal Penalties

- Knowingly using, obtaining or disclosing individually identifiable health information is punishable by criminal sanctions
  - Knowingly obtaining or disclosing individually identifiable health information in violation of HIPAA
    - ≤ 1 year imprisonment and/or ≤ $50,000 fine
  - Knowingly obtaining individually identifiable health information under "false pretenses"
    - ≤ 5 years imprisonment and/or ≤ $100,000 fine
  - Knowingly using or disclosing individually identifiable health information for commercial advantage, personal gain, or malicious harm
    - ≤ 10 years imprisonment and/or ≤ $250,000 fine

Enforcement of HIPAA Privacy Rule

- HHS Office of Civil Rights (OCR) is charged with enforcing HIPAA's Privacy Rule
- Enforcement has been complaint-driven
- More than 20,000 complaints have been received to date by OCR
- No civil monetary penalties have been imposed to date, but at least 3 cases have been filed seeking criminal sanctions:
  - *United States v. Ferrer*, No. 06-CR-60261-CR-Cohn (S.D. Fla.) (indictment filed Sept. 7, 2006)
  - *United States v. Ramirez*, No. 7:05-CR-00708 (S.D. Tex.) (plea agreement Mar. 6, 2006)
  - *United States v. Gibson*, No. CR04-0374 RSM (W.D. Wash.) (plea agreement Aug. 19, 2004)

PROSKAUER ROSE LLP®

PROSKAUER® on PRIVACY

The Latest Developments in Health Privacy

W E B I N A R

November 9, 2006

Presented by:

Sara Krauss
Proskauer Rose LLP
New York, NY
212.969.3049
skrauss@proskauer.com