Privacy and Information Security Law

Randy Canis

CLASS 10

Health Privacy pt. 2; Consumer Data pt. 3
Healthy Privacy pt. 2

Security Rule Basics

• “The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called ‘covered entities’ must put in place to secure individuals’ ‘electronic protected health information’ (e-PHI).”

• http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Security Rule

• Security rules only applies to e-PHI
• Sets forth administrative, physical, and technical safeguards
  – Safeguards are either required or an alternative may be chosen if justified by explanation
Safeguards

• Covered entities must:
  – Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  – Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  – Protect against reasonably anticipated, impermissible uses or disclosures; and
  – Ensure compliance by their workforce.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/sr_summary.html

Defined Security Measures?

• "When a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:
  – Its size, complexity, and capabilities,
  – Its technical, hardware, and software infrastructure,
  – The costs of security measures, and
  – The likelihood and possible impact of potential risks to e-PHI.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/sr_summary.html

Risk Analysis

• Covered entities must perform risk analysis
• A risk analysis process includes, but is not limited to, the following activities:
  – Evaluate the likelihood and impact of potential risks to e-PHI;
  – Implement appropriate security measures to address the risks identified in the risk analysis;
  – Document the chosen security measures and, where required, the rationale for adopting those measures; and
  – Maintain continuous, reasonable, and appropriate security protections.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/sr_summary.html
Information Access Management

- "Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the ‘minimum necessary,’ the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access)."

Physical Safeguards

- "Facility Access and Control. A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.
- Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI)."

Policies and Procedures and Documentation Requirements

- "A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.
- Updates. A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI)."
Breach Notification Rule

- Requires individuals to be notified if their PHI is involved in a data security breach
- Applies to unencrypted PHI
- Must notify affected individuals

Breach

- Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.
- §164.402

Breach Exclusions

- Certain unintentional acquisitions, accesses, or uses of PHI by a workforce member or person acting under the authority of a covered entity or a business associate
- Inadvertent disclosures by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate
- A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- §164.402
Breach Notifications

• §164.404(a) Standard — (1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

Notification Contents

• Brief description of what happened
• Types of unsecured PHI involved
• Steps individuals should take to protect themselves
• A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
• Contact procedures
• § 164.404(c)(1)

Enforcement and Preemption

• Civil penalties – fines of 50K-1.5 million per provision of HIPAA violated
• Criminal penalties – with a malicious motive, personal fines of up to 250K and up to 10 years in jail
• No private right of action
• States can pass more stringent requirements
Parkview Health System, Inc. Resolution Agreement and Corrective Action Plan

• Parkview was receiving a doctor’s medical records
  – “On June 4, 2009, Parkview failed to appropriately and reasonably safeguard the PHI, when Parkview employees, with notice that Dr. Hamilton had refused delivery and was not at home, delivered and left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of Dr. Hamilton’s home, within 20 feet of the public road and a short distance away (four doors down) from a heavily trafficked public shopping venue.”

Parkview Health System, Inc. Resolution Agreement and Corrective Action Plan

• 800K fine
• Corrective Action Plan (CAP)
• Release from HHS only

Parkview Health System, Inc. Resolution Agreement and Corrective Action Plan

• Written policies and procedures
• Provide safeguards
• Reportable events to HHS for violations
• Training
• For 1 year…
HIPAA Complaints

- Most investigated complaints:
  1. Impermissible uses and disclosures of protected health information;
  2. Lack of safeguards of protected health information;
  3. Lack of patient access to their protected health information;
  4. Uses or disclosures of more than the minimum necessary protected health information; and

HIPAA Enforcement

- After HITECH, companies paid significant monetary fines for failure to comply
- Data breaches of more than 500 people are on the HHS wall of shame

Data Breach

- "The HITECH Act defines data breach as ‘the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.’"
Criminal Liability

• “The only mens rea that a person must have for a criminal violation of HIPAA is to know that the data is individually identifiable health information relating to an individual. If a person then accesses it, uses it, or discloses it in violation of HIPAA, it will be a crime.”

REVIEW OF HIPAA PRIVACY RULE

B. CONSTITUTIONAL PROTECTION OF MEDICAL INFORMATION
The Constitutional Right to Privacy

• “Although the U.S. Constitution does not explicitly mention privacy, in a line of cases commonly referred to as ‘substantive due process,’ the Supreme Court has held that there exists a ‘right to privacy’ in the U.S. Constitution.”

Penumbras

• “The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.”
  – 1st – right of association
  – 3rd – prohibition against quartering soldiers
  – 4th – right against unreasonable searches and seizures
  – 5th – right against self incrimination
  – 9th – “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”
• Griswold v. Connecticut, 381 U.S. 479 (1965)

Whalen v. Roe

• Issue
  – Identify patients taking prescription drugs on certain drug schedules
Whalen v. Roe

• "With an exception for emergencies, the Act requires that all prescriptions for Schedule II drugs be prepared by the physician in triplicate on an official form. The completed form identifies the prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient. One copy of the form is retained by the physician, the second by the pharmacist, and the third is forwarded to the New York State Department of Health in Albany. A prescription made on an official form may not exceed a 30-day supply, and may not be refilled."

Whalen v. Roe

• "Appellees contend that the statute invades a constitutionally protected ‘zone of privacy.’ The cases sometimes characterized as protecting ‘privacy’ have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."

Whalen v. Roe

• "[D]isclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy."
Whalen v. Roe

• "We hold that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either the reputation or the independence of patients for whom Schedule II drugs are medically indicated is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment."

Limitations of Government Access

• Whalen provides a judicial recognition that constitutional protection for limited government access about individuals is not limited by explicit constitutional amendments (e.g., the 4th Amendment)

From Whalen

• Decisional privacy - involves the extent to which a state can become involved with the decisions an individual makes with regard to his/her body and family
• "Constitutional right to information privacy" - involves the privacy implications of the collection, use, and disclosure of personal information
Westinghouse Test

- “[The Third Circuit] articulated seven factors that should be considered in deciding whether an intrusion into an individual’s privacy is justified”: (1) ‘the type of record requested’; (2) ‘the information it does or might contain’; (3) ‘the potential for harm in any subsequent nonconsensual disclosure’; (4) ‘the injury from disclosure to the relationship in which the record was generated’; (5) ‘the adequacy of safeguards to prevent unauthorized disclosure’; (6) ‘the degree of need for access’; and (7) ‘whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.”

42 U.S.C. §1983

- Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any state or territory, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit at equity, or other proper proceeding for redress.

§1983 Actions

- Constitutional violations in civil law
- Transforms constitutional violations into tort actions and enables plaintiffs to collect damages and obtain injunctions
- Sue state officials instead of the states directly
State and Local Officials

• “[A]ny state or local official can be sued directly under §1983. State governments cannot be sued. Local governments can be sued, but only when their policy or custom inflicts the injury, not merely because they employ the officials who caused the injury.”

Chaplin Access to Medical Records

• “In allowing chaplains free access to medical records, BMC is not properly respecting a patient’s confidentiality and privacy. The Court concludes that patient medical records can only be accessed by a chaplain upon prior express approval of the individual patient or his guardian.”

Doe v. Borough of Barrington

• Issue
  – Was police office’s disclosure of AIDS related information a violation of a constitutional right of privacy, and therefor actionable under 42 U.S.C. §1983?
Doe v. Borough of Barrington

• "Detective Preen of the Barrington police arrived and, in a private conversation with Van Camp, revealed that Jane Doe's husband had been arrested earlier in the day and had told Barrington police officers that he had AIDS. Van Camp then told defendant Smith. After Jane Doe and Tarvis left the immediate vicinity, defendant Smith told the DiAngelos that Jane Doe's husband had AIDS and that, to protect herself, Rita DiAngelo should wash with disinfectant."

• "This court finds that the Constitution protects plaintiffs from governmental disclosure of their husband's and father's infection with the AIDS virus. The United States Supreme Court has recognized that the fourteenth amendment protects two types of privacy interests. 'One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.' Whalen v. Roe, 429 U.S. 589, 599-600 (1977). Disclosure of a family member's medical condition, especially exposure to or infection with the AIDS virus, is a disclosure of a 'personal matter.'"

• "An individual's privacy interest in medical information and records is not absolute. The court must determine whether the societal interest in disclosure outweighs the privacy interest involved. To avoid a constitutional violation, the government must show a compelling state interest in breaching that privacy. The government's interest in disclosure here does not outweigh the substantial privacy interest involved."
Doe v. Borough of Barrington

- “This court concludes that the Does have a constitutional right of privacy in the information disclosed by Smith and the state had no compelling interest in revealing that information. As such, the disclosure violated the Does’ constitutional rights.”

Prescription Drug Information

- The Supreme Court, in Whalen v. Roe, noted that the right to privacy encompasses two separate spheres. One of these is an individual’s interest in independence in making certain decisions. The other is an interest in avoiding disclosure of personal information. Medical records fall within the second category. Therefore, the Court held that individuals do have a limited right to privacy in their medical records. … An individual using prescription drugs has a right to expect that such information will customarily remain private.”
- Doe v. Southeastern Pennsylvania Transportation Authority, 72 F. 3d 1133 (3rd. Cir. 1995)

Diagnostic Tests

- “The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent … In this case, however, the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment. This fact distinguishes this case from circumstances in which physicians or psychologists, in the course of ordinary medical procedures aimed at helping the patient herself, come across information that under rules of law or ethics is subject to reporting requirements, which no one has challenged here.”
C. GENETIC INFORMATION

Physician and Patient

• "(1) a physician must disclose personal interests unrelated to the patient's health, whether research or economic, that may affect the physician's professional judgment; and (2) a physician's failure to disclose such interests may give rise to a cause of action for performing medical procedures without informed consent or breach of fiduciary duty."

• Moore v. Regents of the University of California

Genetic Information Nondiscrimination Act

• Prevents insurance companies and employers from using genetic tests to deny individuals health coverage or employment
G. FIRST AMENDMENT LIMITATIONS ON PRIVACY REGULATION

1st Amendment Protection of Commercial Speech

- Commercial speech receives constitutional protection
- However, it is of lower value and receives less protection
Constitutionality of Restrictions on Commercial Speech

• “In Central Hudson, 447 U.S. 557 (1980), the Court established a four-part test for analyzing the constitutionality of restrictions on commercial speech:
  • ‘At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.”

Mainstream Marketing Services, Inc. v. FTC

• Issue
  – Is the national do-not-call registry constitutional?

Mainstream Marketing Services, Inc. v. FTC

• Effect of registry
  – “Commercial telemarketers are generally prohibited from calling phone numbers that have been placed on the do-not-call registry, and they must pay an annual fee to access the numbers on the registry so that they can delete those numbers from their telephone solicitation lists.”
Mainstream Marketing Services, Inc. v. FTC

- **Application** – telemarketing, not charitable or political fundraising
- **Exceptions** – established business relationship or express written permission
- 3 months to remove; valid for 5 years

---

Mainstream Marketing Services, Inc. v. FTC

- “The government asserts that the do-not-call regulations are justified by its interests in 1) protecting the privacy of individuals in their homes, and 2) protecting consumers against the risk of fraudulent and abusive solicitation. Both of these justifications are undisputedly substantial governmental interests.”

---

Mainstream Marketing Services, Inc. v. FTC

- “[T]he national do-not-call registry is designed to reduce intrusions into personal privacy and the risk of telemarketing fraud and abuse that accompany unwanted telephone solicitation. The registry directly advances those goals.”
Mainstream Marketing Services, Inc. v. FTC

• "We hold that the national do-not-call registry is narrowly tailored because it does not over-regulate protected speech; rather, it restricts only calls that are targeted at unwilling recipients. … [T]he do-not-call regulations only block calls that would constitute unwanted intrusions into the privacy of consumers who have signed up for the list."

Privacy and Substantial State Interest

• "Therefore, the specific privacy interest must be substantial, demonstrating that the state has considered the proper balancing of the benefits and harms of privacy. In sum, privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it."

• U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999)

Sorrell v. IMS Health, Inc.

• Issue
  – Are the restrictions on the sale of pharmacy records that reveal prescribing practices of individual doctors constitutional?
Sorrell v. IMS Health, Inc.

• "Knowledge of a physician's prescription practices—called 'prescriber-identifying information'—enables a detailer better to ascertain which doctors are likely to be interested in a particular drug and how best to present a particular sales message. Detailing is an expensive undertaking, so pharmaceutical companies most often use it to promote high-profit brand-name drugs protected by patent. Once a brand-name drug's patent expires, less expensive bioequivalent generic alternatives are manufactured and sold."

Sorrell v. IMS Health, Inc.

• "A health insurer, a self-insured employer, an electronic transmission intermediary, a pharmacy, or other similar entity shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use of regulated records containing prescriber-identifiable information for marketing or promoting a prescription drug, unless the prescriber consents...

Pharmaceutical manufacturers and pharmaceutical marketers shall not use prescriber-identifiable information for marketing or promoting a prescription drug unless the prescriber consents."

Sorrell v. IMS Health, Inc.

• "On its face, Vermont's law enacts content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information. The provision first forbids sale subject to exceptions based in large part on the content of a purchaser's speech. For example, those who wish to engage in certain 'educational communications,' §4631(e)(4), may purchase the information. The measure then bars any disclosure when recipient speakers will use the information for marketing. Finally, the provision's second sentence prohibits pharmaceutical manufacturers from using the information for marketing. The statute thus disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers."
Sorrell v. IMS Health, Inc.

• "As a result of these content- and speaker-based rules, detailers cannot obtain prescriber-identifying information, even though the information may be purchased or acquired by other speakers with diverse purposes and viewpoints. . . . For example, it appears that Vermont could supply academic organizations with prescriber-identifying information to use in countering the messages of brand-name pharmaceutical manufacturers and in promoting the prescription of generic drugs. But § 4631(d) leaves detailers no means of purchasing, acquiring, or using prescriber-identifying information. The law on its face burdens disfavored speech by disfavored speakers."

Sorrell v. IMS Health, Inc.

• Justifications
  – Necessary to protect medical privacy
  – Policy objectives – improved public health and reduced healthcare costs

Sorrell v. IMS Health, Inc.

• "The explicit structure of the statute allows the information to be studied and used by all but a narrow class of disfavored speakers. Given the information’s widespread availability and many permissible uses, the State’s asserted interest in physician confidentiality does not justify the burden that §4631(d) places on protected expression."
Sorrell v. IMS Health, Inc.

- “[T]he State does not explain why detailers’ use of prescriber-identifying information is more likely to prompt these objections than many other uses permitted by §4631(d). In any event, this asserted interest is contrary to basic First Amendment principles. . . . If pharmaceutical marketing affects treatment decisions, it does so because doctors find it persuasive. Absent circumstances far from those presented here, the fear that speech might persuade provides no lawful basis for quieting it.”