Privacy and Information Security Law

Elizabeth Ortmann-Vincenzo

CLASS 5

Health Privacy

Part 1

About me

Elizabeth Ortmann-Vincenzo

Healthcare industry since 1994

Health lawyer since 2002

Experience:

- Magellan Behavioral Health
- Wyeth Pharmaceuticals
- Johnson & Johnson (Centocor Division)
- American Optometric Association
- Private law firms
- Express Scripts

2

CONFIDENTIALITY OF HEALTH INFORMATION

U.S. Historical Information

- Prior to 20th century: Physician Ethics and Loose, voluntary guidelines and common practice
- Most of 20th century: Confusing array of constitutional, common law, and statutory rules, often based on general evidentiary principles
- Last quarter of 20th century
  - Case law
  - HIPAA
- 21st Century
  - HITECH
  - Explosion of state law

3

Oath and Law of Hippocrates (c. 400 B.C.)

- "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."

4

Medical Ethics & Common Law

- Pre-condition: Formation of physician-patient relationship
- AMA Canons
- State ethics laws under the jurisdiction of the body overseeing physician licensure
- Evidentiary privileges
- Common law causes of action:
  - Breach of contract (contract)
  - Medical Malpractice (tort)
  - Breach of Fiduciary Duty (tort)
  - Privacy Torts

5

Basic Evidentiary Privileges

- (1) **spousal privilege** whereby a person can refuse to testify against his or her spouse in a criminal case; (2) **spousal privilege** in preventing one's spouse or former spouse from disclosing marital communications in criminal or civil cases; (3) **accountant-client privilege**; (4) **priest-penitent privilege**, whereby a person can prevent the disclosure of confidential communications made when seeking spiritual advice from his or her clergy member; (5) **physician-patient privilege**; (6) **voter privilege**, whereby a person can refuse to testify as to how he or she voted in any political election; (7) **journalist privilege**, where journalists can refuse to divulge information sources; and (8) **executive privilege**, permitting the President of the United States from divulging secrets necessary to the carrying out of his or her constitutional functions.

6

Exceptions to Confidentiality

- "… We conclude, therefore, that ordinarily a physician receives information relating to a patient's health in a confidential capacity and should not disclose such information **without the patient's consent**, except where the **public interest** or the **private interest of the patient** so demands. …"
- Hammonds v. Aetna Casualty & Surety Co., 243 F. Supp. 793 (D. Ohio 1965)

7

Exceptions to the Tort

- "One important exception to the tort is that physicians will not be liable for disclosing confidential medical information **when it is necessary to protect others from danger or when it is required by law**."
- Mandatory Reporting Laws

8

Seminal Case Law: Tarasoff v. Regents of University of California

- Issue
  - Does a psychologist owe a duty of care to a potential victim of a patient in the psychologist's care?

9

Tarasoff v. Regents of University of California

- "We shall explain that defendant therapists cannot escape liability merely because Tatiana herself was not their patient. When a therapist determines, or pursuant to the standards of his profession should determine, that his patient presents a serious danger of violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger. The discharge of this duty may require the therapist to take one or more of various steps, depending upon the nature of the case. Thus it may call for him to warn the intended victim or others likely to apprise the victim of the danger, to notify the police, or to take whatever other steps are reasonably necessary under the circumstances. …"

10

Tarasoff v. Regents of University of California

- "As a general principle, a "defendant owes a **duty of care** to all persons who are **foreseeably endangered by his conduct**, with respect to all risks which make the conduct unreasonably dangerous." … [W]hen the avoidance of foreseeable harm requires a defendant to control the conduct of another person, or to warn of such conduct, the **common law has traditionally imposed liability only if the defendant bears some special relationship to the dangerous person or to the potential victim**. Since the **relationship between a therapist and his patient satisfies this requirement**, we need not here decide whether foreseeability alone is sufficient to create a duty to exercise reasonable care to protect a potential victim of another's conduct."

11

Protection of Intended or Potential Victim

- "[T]his court holds that a psychiatrist or therapist may have a **duty to take whatever steps are reasonably necessary to protect** an intended or potential victim of his patient when he determines, or should determine, in the appropriate factual setting and in accordance with the standards of his profession established at trial, that the patient is or may present a probability of danger to that person. The relationship giving rise to that duty may be found either in that **existing between the therapist and the patient**, as was alluded to in *Tarasoff*, or in the more broadly based **obligation a practitioner may have to protect the welfare of the community**, which is analogous to the obligation a physician has to warn third persons of infectious or contagious disease."

12

HIV Notification Statutes

- Some states have partner notification laws
- "According to N.Y. Pub. Health L. § 2130, an HIV-positive diagnosis shall be reported to public health officials. The report "'shall include information identifying the protected individual as well as the names, if available, of any contacts of the protected individual … known to the physician or provided to the physician by the infected person.'"

13

Other Disclosure Requirements

- Many states have statutory requirements for physicians to disclose health information for certain types of diseases or injuries.
- Collection of certain medical data relating to public health issues, such as birth defects, cancer, occupational diseases, infectious diseases, health injuries related to possible child abuse, gun shot wounds, etc.

14

State Law Privacy Protections for Medical Information

- Some state regulation of personal information beyond Federal Laws
- "Disclosure of medical information can give rights to a claim for public disclosure of private facts."
- Certain states have recognized tort liability when physicians disclose a patient's medical information.

15

State Law Privacy Protections for Medical Information

- **Mandatory report laws** – "require that medical personnel or institutions report certain health information to state agencies or to others"
- **Research disclosure laws** – "regulate the use of medical data for research purposes"
- **Medical confidentiality laws** – "specific statutes providing civil and criminal protection against the disclosure of medical information"
- **Patient access laws** – right to access certain medical records

16

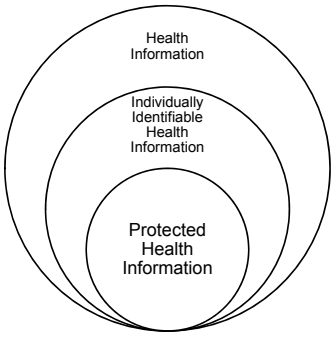
HIPAA

17

HIPAA

- What is HIPAA?
  - Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule
    - addresses the use and disclosure of individuals' health information
  - Security Rule
    - Requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address them

18



19

Information Hierarchy

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually Identifiable Information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI) is all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media

20

HIPAA Applicability: Covered Entities

- A "**health care provider**" is a "provider of medical or health services . . . and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103. Examples of health care providers are physicians, hospitals, and pharmacists.
- A "**health plan**" is "an individual or group plan that provides, or pays the cost of, medical care." 45 C.F.R. § 160.103. This definition encompasses health insurers and HMOs.
- A "**health care clearinghouse**" is a public or private entity that processes health information into various formats — either into a standard format or into specialized formats for the needs of specific entities. 45 C.F.R. § 160.103.

21

Covered Entity Responsibilities

- Privacy Officer
  - Designated by the company
  - Responsible for implementation of privacy policies and procedures
  - Designated to receive complaints
- Notice of Privacy Practices
- Risk Assessments
- Breach Notification

22

Covered Entity Responsibilities

- Written policies and procedures
- Training for workforce members
- Appropriate safeguards to protect PHI
- Observe Individuals' rights: amendment, accounting of disclosures, access, restrictions, communication preferences

23

General Use and Disclosure

- A covered entity may only use PHI as permitted under the Privacy Rule
  - Uses and disclosures to carry out treatment, payment, or health care operations.
  - Uses and disclosures for which an authorization is required.
  - Uses and disclosures requiring an opportunity for the individual to agree or to object.
  - Uses and disclosures for which an authorization or opportunity to agree or object is not required

24

TPO

- Treatment
- Payment
- Healthcare Operations

25

Authorization Required

- Disclosure of psychotherapy notes
- Marketing
- Sale of PHI
- Otherwise not covered by Privacy Rule
- Elements of an Authorization

26

Must Provide an Opportunity to Object

- Emergencies
- To persons involved in an individual's care
- When the Individual is present
- When the Individual not present
- Disaster Relief
- Deceased Individuals

27

Provision of Opportunity to Object Not Required

- Public Health
- Law Enforcement
- Abuse, neglect, domestic violence
- Health oversight
- Failure to notify an Individual
- Health oversight
- Judicial Proceedings
- Decedents
- Disclosure by HCP in an emergency
- Research
- Military or Veterans
- "Good Faith"
- National Security
- Protective services (e.g., POTUS)
- Medical suitability
- Correctional institutions
- National Criminal Background Check System
- Public Benefits

28

Other HIPAA Topics: De-Identified Health Information

- Health information that neither identifies nor provides a reasonable basis to identify an individual
- No restrictions on use or disclosure under HIPAA

29

Other HIPAA Topics

- Limited Data Sets
- Fundraising
- Underwriting

30

Business Associates

- A **business associate** is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
- From HHS Summary of the HIPAA Privacy Rule

31

Business Associate Functions and Activities

- Claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

32

Business Associate Services

- Legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial

33

Business Associate Agreement

- A covered entity needs a business associate agreement with another company that is providing “business associate” services on its behalf
- Business associate agreement must be in writing and provide for safeguarding of individually identifiable health information provided by the covered entity to the business associate

34

Required Agreement Elements

- Describe the **permitted and required uses** of PHI by the business associate;
- Provide that the business associate will not use or further disclose the PHI **other than as permitted** or required by the contract or as required by law; and
- Require the business associate to use **appropriate safeguards** to prevent a use or disclosure of the PHI other than as provided for by the contract.

35

Class 10: 10/25/16

- HIPAA Security Rule
- HIPAA Enforcement and Liability
- State Health Privacy
- Constitutional Right to Privacy
- Genetic Information

36

Program Completed

37