Beliefs, Determinations and Agreements: Contextualizing Privacy in Practice

Travis D. Breaux, PhD Candidate
North Carolina State University
tdbreaux@ncsu.edu

Carolina Privacy Officials Network, January 29, 2008

Problem and Motivation

- Health Insurance Accountability and Portability Act (HIPAA) Privacy Rule governs access to medical information
- HIPAA is limited to electronic patient health information
- HIPAA Privacy Rule affects 545,000 establishments who employ 13.5M people
- Projected HIPAA compliance costs: $12-$42B

In software engineering, verification begins by understanding the software requirements

Compliance Goals

- *Due diligence* refers to reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations
- *Standard of care* means "under the law of negligence or of obligations, the conduct demanded of a person in a situation; typically, this involves a person giving attention both to possible dangers, mistakes and pitfalls and to ways of minimizing those risks."

Black's Law Dictionary, 8th ed.

Identifying Legal Requirements

permissions, obligations and constraints

(1) The covered entity who has a direct treatment relationship with the individual **must**…

(A) Provide notice no later than the first service delivery;

(2) For the purposes of paragraph (1), a covered entity who delivers services electronically **must** provide electronic notice **unless** the individual requests to receive a paper notice.

Important keywords are **bold**

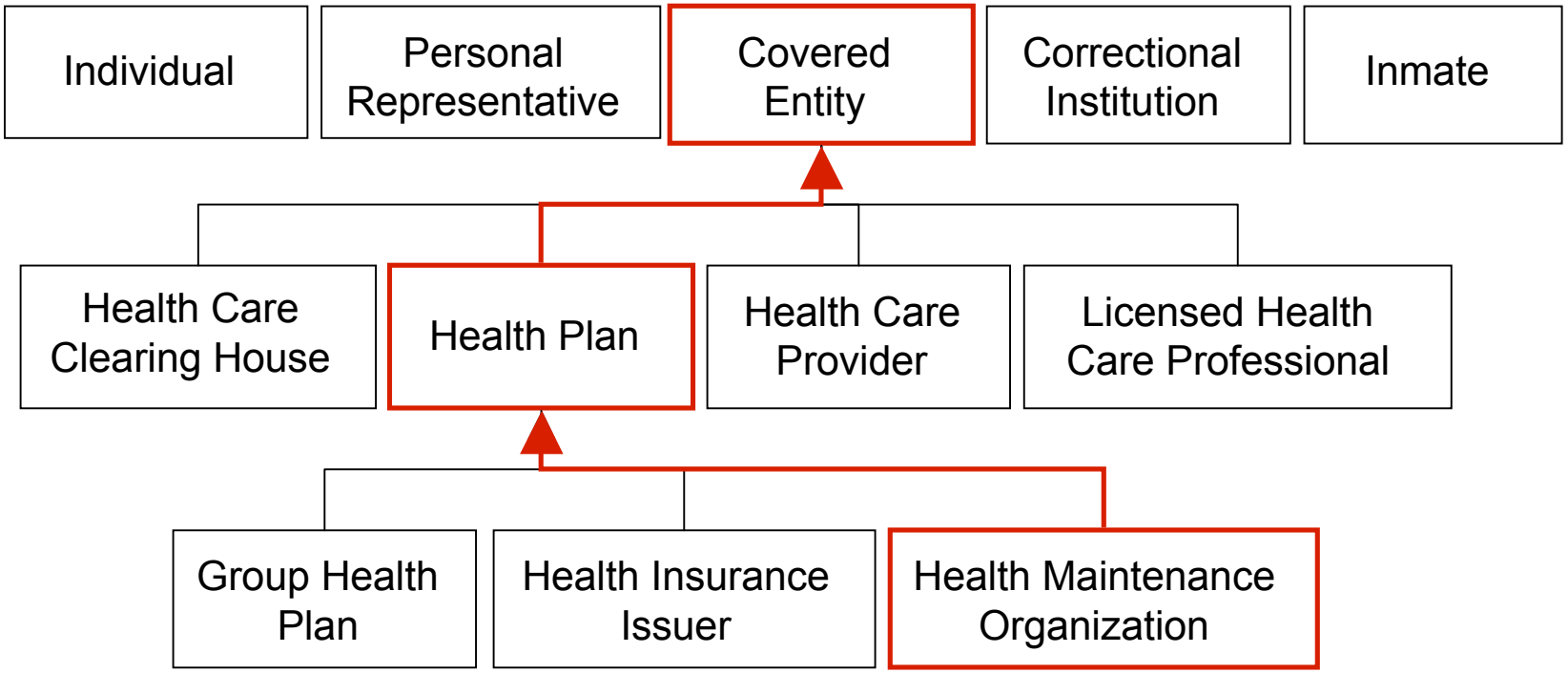
Obligations are red

Constraints are underlined

From HIPAA §160.520

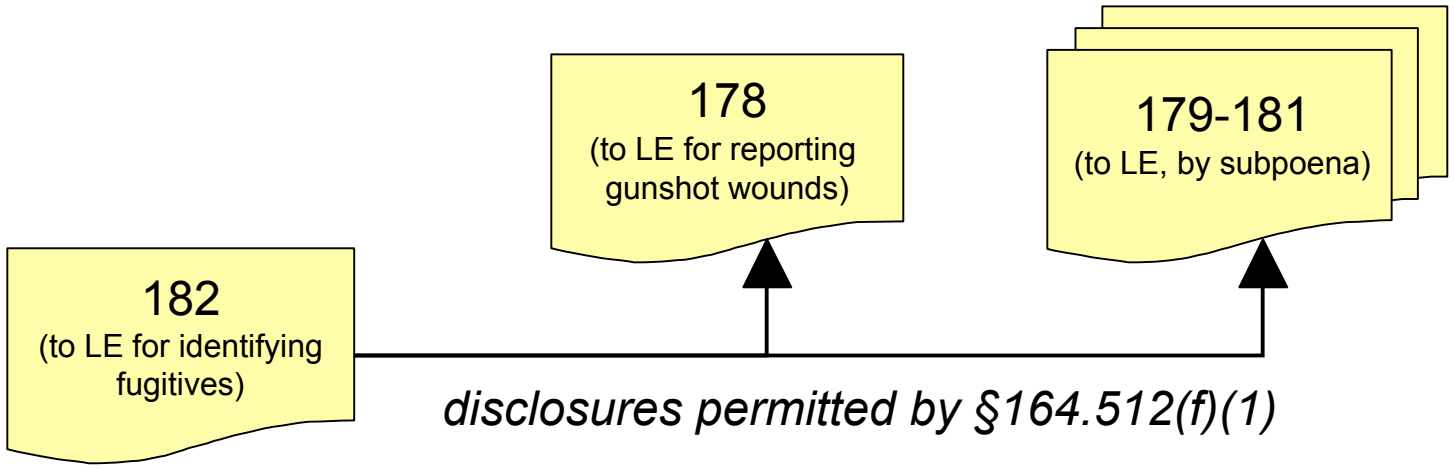
Stakeholder Classification Hierarchy
definitions

- Stakeholders must satisfy all of the obligations in their classification hierarchy.

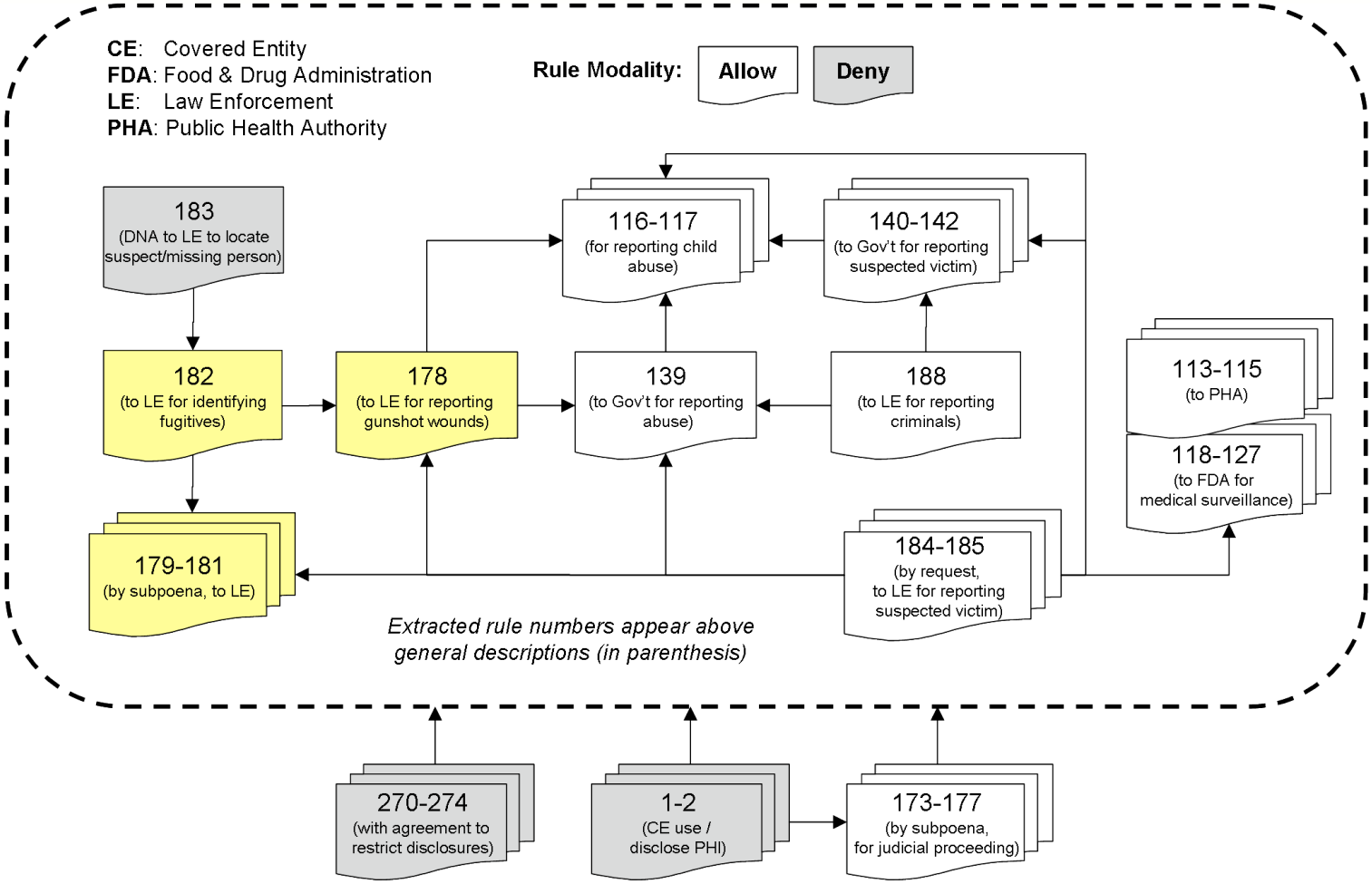


Requirements Priority Hierarchies

HIPAA §164.512(f)(2): *Except for disclosures required by law as permitted by paragraph 164.512(f)(1),* a covered entity may disclose PHI in response to a law enforcement (LE) official's request for the purpose of identifying or locating a suspect



Requirements Priority Hierarchies



HIPAA Case Study
privacy rule

- Identified over 300 information access requirements (legal uses and disclosures)

Constraints on Information Access	Total
Legal Determinations	231
Medical Determinations	184
Personal Beliefs	71
Contractual Statements	170
Data Subjects	42
Data Purposes	389

Appears in 2008 Jan/ Feb Issue of IEEE TSE

Beliefs and Determinations

legal determinations

1. Who needs the PHI to comply with its obligations under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose.
2. Who has lawful custody of an inmate or individual.
3. Who is authorized by law to receive reports of child abuse or neglect.
4. Who treats the individual as required by law.
5. Who are authorized by 18 U.S.C. 3056.
6. Who is authorized by law to notify persons to conduct public health interventions.

Beliefs and Determinations

medical determinations

1. Who determines the use and disclosure is necessary to respond to an emergency circumstance.
2. Who may have been exposed to a communicable disease.
3. Which concerns a work-related illness or injury.
4. Who determines the individual is incapacitated.
5. Who represents that the PHI is necessary for the health and safety of such individual or other inmates.
6. Which an LHP determines is reasonably likely to endanger the life or physical safety of the individual.

Beliefs and Determinations

personal beliefs

1. Who believes in good faith the CE engaged in unlawful conduct, violates professional standards, or potentially endangers others.
2. Who determines the consent of the individual is inferred from the circumstances.
3. Who determines the disclosure is in the best interest of the individual.
4. Who determines the individual is not present.
5. Who believes the individual of the PHI is a victim of abuse, neglect or domestic violence.
6. Who believes the PHI constitutes evidence of criminal conduct on the premises of the CE.

Beliefs and Determinations

contractual statements

1. Who attempts to obtain satisfactory assurances in a memorandum or contract with the Business Associate.
2. Who has obtained the consent of the individual for the disclosure.
3. Who obtains a valid authorization.
4. Who obtains an alteration or waiver of an individual's required authorization.
5. Who has an agreement with an individual to restrict disclosures of PHI.
6. Who agrees to the fees imposed for the summary of the PHI.

Beliefs and Determinations

data subjects

1. Which is about the suspected perpetrator of the criminal act.
2. From an individual who is an inmate.
3. Which is about an individual who has died.
4. About individuals who are Armed Forces personnel.
5. About individuals who are Armed Forces personnel who have been separated or discharged from military service.
6. Who receives a request from the law enforcement official to receive PHI about an individual who is or is suspected to be a victim of a crime.

Beliefs and Determinations

data purposes

1. Which can be used to re-identify de-identified PHI.
2. Which is compiled for use in a civil, criminal or administrative proceeding.
3. For alerting law enforcement to the death of the individual.
4. For marketing.
5. Who administers a government program providing public benefits.
6. Who is engaged in procurement, banking, or transplantation of cadaveric organs, eyes, or tissue.

Questions?

- T.D. Breaux, A.I. Antón. “Analyzing Regulatory Rules for Privacy and Security Requirements” Appears in the *IEEE Transactions on Software Engineering*, v. 34, n. 1, pp. 5-20, January 2008.