Data Privacy in Biomedicine
Lecture 2: Ideology, Law, & Regulation

Bradley Malin, PhD  (b.malin@vanderbilt.edu)
Professor of Biomedical Informatics, Biostatistics, & Computer Science
Vanderbilt University
January 8, 2020

© 2020 Bradley Malin

What is Privacy?

- Freedom from Intrusion
- Public-Private Divide / Body Privacy
- Communications Privacy
- Identity Management
  - Information privacy
  - Survival value of information
  - Individual facts vs. collected knowledge
  - Surveillance

Legal Aspects of Privacy

- United States
  - Federal / State level
  - Privacy Act of 1974
  - Privacy on the WWW
  - Educational (FERPA)
  - Financial (GLB)
  - Medical (HIPAA)
  - Minors (COPPA)
  - Wiretap and Surveillance Laws
  - HIPAA
- International
  - EU Data Protection Directive 95/46
  - EU General Data Protection Regulation (GDPR)
  - Safe Harbor and US (now Privacy Shield)
  - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Today’s Topics

- Laws & Ideologies in the US
- Laws & Ideologies in the EU
- Health, Hippocrates, and HIPAA

Models of Data Protection (1)

- Sectorial laws:
  - Different rules for different sectors (e.g., financial information, medical records)
    - adopted in USA
- Comprehensive laws:
  - General laws governing collection, use and dissemination of data and an oversight body
    - adopted by EU
  - Variation: coregulatory model
    - Canada, Australia
    - Industry develops rules

Models of Data Protection (2)

- Self-regulation:
  - Code of practice
  - Code of conduct
- Technology for privacy:
  - Exploitation of technology for privacy protection
    - Example: encryption
The Warren & Brandeis Model

- Couple of Harvard Law grads from late 1800s
- Founded Boston law firm Nutter, McClennen, and Fish (it’s still around)
- Brandeis went on to the Supreme Court for 23 years (1916 – 1939)
- Warren went on to a very high-profile marriage to Mabel Bayard
  - Daughter of Thomas F. Bayard: 3 time senator of Delaware, U.S. Secretary of State, U.S. Ambassador to the U.K.

Brandeis & the US Supreme Court

- Olmstead v. U.S. (1928)
  - Case: People were convicted for an alleged conspiracy to violate the National Prohibition Act
  - An additional 72 people were indicted based on telephone conversations
  - Overwhelming evidence
    - Roy Olmstead, general manager (50% of profits)
    - 56 employed people
    - Proof of sea vessels for transporting bootleggers and alcohol
    - Underground storage facility in Seattle
    - Central office with executives, accountants, salesmen, and... an attorney

4th Amendment to the US Constitution

- Protection from illegal search and seizure
- Protects against government intrusion into private life
  - Goal: Prevent the suppression of peaceful political dissent
  - “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

5th Amendment to the US Constitution

- Famous for “I plead the 5th”
- Principle interest is that you do not incriminate yourself
- Requirement for “due process”
  - Government must adhere to a person’s legal rights
Brandeis & the US Supreme Court

- Olmstead v. U.S. (1928)
  - Official Ruling: No (majority opinion delivered by Chief Justice Taft)
  - Brandeis offered the minority opinion:
    - Argued that the “right to privacy” was protected under the U.S. Constitution
    - “most comprehensive of rights”
    - “right most valued by civilized men”
    - Based on a little something he wrote almost 40 years earlier

What is Privacy?

- Freedom from intrusion
  - Brandeis and Warren (1890): Right to be left alone
    1. “does not prohibit any publication of matter which is of public or general interest”
    2. “does not prohibit the communication of any matter … [that is] privileged communication”
    3. “[does] not grant any redress for the invasion of privacy by oral publication in the absence of special damage”

A Broader Perspective

- Prosser (1960) organized the concept of privacy into four distinct torts, or “civil wrongs”:
  - Violation of solitude, solitude, or private matters
  - Public disclosure of facts that are, or could be embarrassing
  - Publicity that puts an individual in a false light to the public
  - Misappropriation of name or likeness

A Conceptual Perspective

- Solitude: Just leave me alone
- Confidentiality: We agree to share information, but only with trusted entities
- Reserve: The creation of a psychological barrier against unwanted intrusion
- Anonymity: I don’t want you to know who I am

Privacy Law & Policy in the US

- Federal: Financial, educational, genetic / medical, children

  - Federal Privacy Act of 1974
    - Applies to personal information collected by the federal government
    - Provides three core rights:
      - The right to see records about yourself (there are exemptions)
      - The right to amend records that are inaccurate
      - The right to sue the government if it violates the act
    - Pertains to information on individuals collected by the government and stored in a “system of records”
      - Does not apply to information that is “filed” under other subjects

**Freedom Of Information Act (FOIA)**

- Established in 1966 (most recently amended in 2002)
- Ensures public access to government records
- U.S. government agencies are required to disclose records, upon written request... unless it can be shown that such records can be lawfully withheld via one of nine exemptions
  - Matters of national defense & foreign policy
  - Internal personnel rules & practices
  - Information exempted by other statutes
  - Trade secrets, commercial, or financial information
  - Privileged interagency or intra-agency communications
  - Personal information affecting an individual’s privacy
  - Records compiled for law enforcement purposes
  - Records of financial institutions
  - Geological and geophysical information concerning wells

**Privacy Law & Policy in the US**

- **Federal:** Financial, educational, genetic / medical, children
- **Bill of Rights:** “liberty” as right to privacy
- **State:** Limited, usually concerned with embarrassing facts
- **State constitutions:**
  - CA: “All people are by nature free and independent and have inalienable rights. Among these are...pursuing and obtaining safety, happiness, and privacy”
  - HI: “The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest”

**Gramm-Leach-Blilley (1999)**

- Financial institutions have continuing obligation to
  - respect privacy of customers
  - protect security and confidentiality of nonpublic personal information
- Protects consumers
  - individual who obtains financial products or services
  - used primarily for personal, family, or household purposes
- No disclosure to unaffiliated third party without notice to the consumer
- Opt-out
  - Consumer may elect to refuse disclosure
  
**COPPA (1998)**

- Children’s Online Privacy Protection Act
- Age < 13 years old
- Online service operator may not collect personal information from a child
  - Unless verifiable parental consent for the collection, use, and/or disclosure
- Exception: Data for 1-time use

**Privacy on the Internet**

- Posted privacy policies ≡ legal representations
- U.S. Federal Trade Commission (FTC) acts on behalf of consumers
  - Wasn’t meant to be this way, but alas
- Violation of privacy policy by a website
  - deceptive advertising
  - unfair trade practice
  
http://business.ftc.gov/privacy-and-security
Data Privacy in Biomedicine: Lecture 2

FERPA (Buckley Amendment)

- **Family Educational Right to Privacy**
- Applies to: schools receiving funds from US Department of Education
- If school permits the release of students’ educational records without written consent of parents → Federal funding refusal to the school
- Parents and eligible students have rights
  - Inspect student’s school's education records
  - Request school correct records believed to be inaccurate or misleading

Privacy in the European Union

- Less notion of personal data as a commodity to be bought and sold (in contrast to US)
- As such, public information is highly restricted
- Conceptually:
  - Prior notice and consent by individual
  - Use restricted to disclosed use
  - Right to access and correction
  - Restricted downstream transfer

EU Privacy Directive

- Full name: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
- Blanket directive for all member states of EU, but are not legally binding for its citizens
- Each state must define its own law based on the Directive and implement additional controls and management structures at it sees fit

Today’s Topics

- Laws & Ideologies in the US
- Laws & Ideologies in the EU
- Health, Hippocrates, and HIPAA

Myhealth Example

http://www.myhealthatvanderbilt.com

https://registrar.vanderbilt.edu/ferpa/
The EU data protection directive (95/46/EC)

- Individuals are provided with certain rights:
  - The right to know where the data originated
  - The right to have inaccurate data rectified
  - The right of recourse in the event of unlawful processing
  - The right to withhold permission to use data in certain circumstances

EU 95/46/EC: Meeting the Rules

- Personal data is any information that can be traced directly or indirectly to a specific person
- Use allowed if:
  - Unambiguous consent given
  - Required to perform contract with subject
  - Legally required
  - Necessary to protect vital interests of subject
  - In the public interest, or
  - Necessary for legitimate interests of processor and doesn’t violate privacy

The Relevant (to Technology) Definitions (1)

- Definition (a):
  "personal data" shall mean any information relating an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

EU 95/46/EC: Meeting the Rules

- Some uses specifically proscribed
  - Can’t reveal racial/ethnic origin, political/religious beliefs, trade union membership, health/sex life
- Must make data available to subject
  - Allowed to object to such use
  - Must give advance notice / right to refuse direct marketing use
- Limits use for automated decisions (e.g., creditworthiness)
  - Person can opt-out of automated decision making
  - Onus on processor to show use is legitimate and safeguards in place to protect person’s interests
  - Logic involved in decisions must be available to affected person

US/EU Agreement on Safe Harbor

- Set of principles which US company may agree
- Safe harbor companies deemed to protect data adequately
  - May be supplied data from EU
  - Need no prior approval of member states
- Claims brought by EU citizens against US companies will be heard in US
  - Enforcement in the US by the FTC and DOT
  - Does not include financial institutions

Safe Harbor Principles (Basis of what is now PrivacyShield)

- Notice
  - "clear and conspicuous" first time data is collected
  - Purpose of collection
  - How to file a grievance
  - Types of 3rd parties with whom data will be shared
- Choice
  - Almost always opt-out
  - Opt-in for sensitive information
- Downstream sharing
- Security
- Data integrity
  - Reliability and consistency with defined purpose
- Access and the right to correct
- Enforcement
  - Recourse
  - Obligation to remedy

Seven Principles
What Happened?

- Comes from 2013 complaint by Austrian privacy activist Max Schrems over Facebook compliance
  - based on Snowden suggestion that Facebook shared data with National Security Agency
- Irish Data Protection Authority (EU base of Facebook) initially rejected complaint
- European Court of Justice ruled otherwise
- Not an immediate end to data transfer
- Gives national regulators the right to investigate and suspend operations of protections are insufficient

Article 29 Working Party Opinion (April 2014)

- Do not rely on the "release and forget" approach.
  - Given residual risk of identification, data controllers should:
    - Identity new risks and re-evaluate the residual risk(s) regularly,
    - Assess whether the controls for identified risks suffice and adjust accordingly; AND
    - Monitor and control the risks
- Context is important
  - Consideration should be given to possible attackers by taking account of the appeal of the data for targeted attacks (again, sensitivity of the information and nature of the data will be key factors in this regard)
- Details on differential privacy, generalization, and more

European Medicines Agency Steps In (October 2014)

- Promulgated recent policy on sharing clinical trials data
- Protect and foster public health, while ensuring there is transparency in clinical trials (which are increasingly based on biomarkers)
  - "The secondary analysis of personal data will have to be fully compatible with the individual privacy of clinical trial participants and data protection"
  - "[recipients of the data will] not seek to re-identify the trial subjects or other individuals from the Clinical Reports in breach of applicable privacy laws"

General Data Protection Directive (GDPR)

- "The GDPR supersedes the Data Protection Directive and will fully phase out the DPD and become national law for all EU Member States by May 25, 2018. The GDPR builds on the key tenets of the DPD with more specific data protection requirements, a global scope, and stiffer enforcement as well as non-compliance penalties."

Today's Topics

- Laws & Ideologies in the US
- Laws & Ideologies in the EU
- Health, Hippocrates, and HIPAA
Hippocratic Oath

- CONFIDENTIALITY: “Whatever in connection with my professional practice or not in connection with it I may see or hear in the lives of my patients which ought not to be spoken abroad, I will not divulge, reckoning that all such should be kept secret.”

- DO NO HARM: “Except for the prudent correction of an imminent danger, I will neither treat any patient nor carry out any research on any human being without the valid informed consent of the subject or the appropriate legal protector thereof, understanding that research must have as its purpose the furtherance of the health of that individual. Into whatever patient setting I enter…”

HIPAA (1996)
(Health Insurance Portability & Accountability Act)

- Rationale: Inconsistent state laws causing unnecessary difficulties in standardization, transfer, & sharing of health information
  - Privacy Rule (went into effect April 14, 2003)
- A covered entity may not use or disclose protected health information (PHI)
- Exceptions
  - To the individual that the information corresponds
  - With consent: to carry out treatment, payment, or health care operations
  - If consent is not required: same as above, but not with respect to psychotherapy notes

HIPAA Definitions

- Health Information: Any information, whether oral or recorded in any form or medium that...
  - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; AND
  - 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 of provision of health care to an individual

- Protected Health Information (PHI)
  - Individually identifiable health information
  - Identifiable corresponds to data that is “explicitly” linked to a particular individual
    - But also includes health information that includes data which could reasonably be expected allow individual identification

Covered Health Care Provider?

- Does the person, business or agency furnish, bill, or receive payment for health care in the normal course of business?
  - Yes: Not a covered health care provider
  - No: It is a covered health care provider

- Does business / agency perform the function for another legal entity?
  - Yes: Not a covered health care provider
  - No: It is a covered health care provider

What is a Clearinghouse?

- Does business / agency perform the processing of, health information from non-standard into standard format or content vice versa?
  - Yes: Not a covered health care provider
  - No: It is a covered health care provider

- Does business / agency perform the function for another legal entity?
  - Yes: It is a covered health care provider
  - No: Not a covered health care provider
And More

- Look online for other fun-filled adventures, including:
  - "Is a private benefit plan a health plan?"
    and
  - "Is a government-funded program a health plan?"


HIPAA – Data Protection

**PRIVACY RULE (2002)**

**SECURITY RULE (2003)**

HIPAA Patient Rights

- Notice of practices that state the uses of, and protections for, PHI
- Obtain copy of health records
- Amend (though not necessarily correct) health records
- An accounting of disclosures made for purposes other than treatment, payment, and healthcare operations (Note: research is different)

Covered Entity Responsibilities

- Provide notice of information practices (not to mention abide by them)
- Designate an individual to be responsible for privacy protection
- Provide "administrative", "physical", and "technical" safeguards for PHI
- Only use / disclose PHI according to HIPAA Privacy Standard
- Agreements with PHI-receiving "business associates" that specify protection measures

HIPAA - Secondary Data Sharing

- Limited Release (Limited Data Set)
- Safe Harbor (A DIFFERENT ONE!)
- Statistical or Scientific Standard

HIPAA’s Safe Harbor

- Data that can be given away by a covered entity
  - Requires removal of eighteen direct and other “quasi-identifiers”
    1) Name / Initials
    2) Street address, city, county, precinct code and equivalent geocodes for ZIP-3 when population is of size < 20,000 people
    3) Dates (indicative of a time period smaller than 1 year) and all ages over 89
    4) Telephone Numbers
    5) Fax Numbers
    6) Electronic Mail Address
    7) Social Security Number
    8) Medical Record Number
    9) Health Plan ID Number
HIPAA’s Safe Harbor

- Safe Harbor (cont’d)
  10) Account Number
  11) Certificate / License Number
  12) Vehicle identifiers and serial numbers, including license plate numbers
  13) Device Identifiers and serial numbers
  14) Web addresses (URLs)
  15) Internet IP Addresses
  16) Biometric identifiers, including finger and voice prints
  17) Full face photographic images and any comparable images
  18) Any other unique identifying number, characteristic, or code

  ◼ A code is an identifier if the person holding the coded data can re-identify
  the individual

*** Must have no actual knowledge the remaining data can be used to identify

Safe vs. Limited

- Name / Initials
- Street address, city, county, precinct code and equivalent geocodes for populations > 20K in size
- Dates smaller than one year and all ages over 89
- Telephone Numbers
- Fax Numbers
- Electronic Mail Address
- Social Security Number
- Medical Record Number
- Health Plan ID Number
- Account Number
- Certificate / License Number
- Vehicle identifiers and serial numbers
- Device Identifiers and serial numbers
- Web addresses (URLs)
- Internet IP Addresses
- Biometric identifiers
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

HIPAA Limited Data Set

- Includes potentially identifiable information

- Can include
  - Dates of (birth, death, service, …, anything)
  - Town or city
  - State
  - Zip code

- Requires Contract: Research entity provides assurances that it will not use or disclose the information for purposes other than research and will not identify or contact the individuals who are the subjects

HIPAA Statistical / Scientific Standard

- Certify via “generally accepted statistical and scientific principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information.”

  - “Must document the methods and results of the analysis that justify such a determination”

  - “Must not disclose the key or other mechanism that would have enabled the information to be re-identified”
    - includes pseudo-random number algorithms and seed values

The Common Rule

- Federal Policy for the Protection of “Human Subjects”
  - http://www.hhs.gov/ohrp/humansubjects/commonrule/

- Agreed upon by over 15 federal agencies

- Human Subject
  - “A living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.”

What about Research?

- HIPAA corresponds to information generated during healthcare

- Does this pertain to information collected for research?
The Long Road to Revision

- 2011 – Advanced Notice for Proposed Rule Making
  - Considers making all biospecimens and derived data “identifiable”
  - Require consent for all collection, use, and reuse
- 2015 – Notice for Proposed Rule Making
  - Considers managing biospecimens via consent
  - Consent allows for specimen collection for 10 years
  - Data derived from biospecimens will not be governed by consent
- 2017 – Final Rule made (on Obama’s last day!)
  - Biospecimens retained their de-identified status

Funding Agency Policy

- “data intended for broader use should be free of identifiers that would permit linkages to individual research participants and variables that could lead to deductive disclosure of the identity of individual subjects”
- “When data sharing is limited, applicants should explain such limitations in their data sharing plans”

Institutional Review Boards (IRBs)

- Primary role is the protection of human subjects.
- Reviews and monitors biomedical and behavioral research
- Composition (sketch)
  - Minimum of 5 members, with representation for both genders, such that there is sufficient expertise to make informed decisions on whether research is ethical and safeguards exist
  - If study includes members of “vulnerable” populations, then a member of such a population should participate on the IRB
  - Members can not all be of same profession
  - Must be at least one person not affiliated with the organization (i.e., the “community” member)
  - Must be at least one scientist AND one non-scientist

Institutional Review Boards (IRBs)

- Minimal requirement for IRB Approval is when research is federally funded – but the organization can impose IRB oversight whenever it believes it is necessary.
- Exemptions to oversight will be provided if the data is believe to be sufficiently anonymous.

Contour of Health Information Access in the US

- HIPAA - Safe Harbor / Statistical Standard
- Common Rule – Non-human subjects
- Limited Data Set
- IRB Approval

Readings for Next Lecture

Required

Optional