2nd Quiz of BME2133 Fall2025

- Covers lectures 4-7;
- 20 minutes;
- 10 multiple-choice questions; and
- 1 essay question (No word limit. 6 sentences recommended. You can use both English (preferred) and Chinese to answer.)

Medical Data Privacy and Ethics in the Age of Artificial Intelligence

Lecture 8: Privacy laws and regulations for biomedical data in the West

Zhiyu Wan, PhD (wanzhy@shanghaitech.edu.cn)
Assistant Professor of Biomedical Engineering
ShanghaiTech University

October 29, 2025

Learning Objectives of This Lecture

- Know key concepts in HIPAA (USA)
- Know key concepts in GDPR (European Union)

Models of Data Protection Laws

- 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, China
  - Variation: coregulatory model
    - Canada, Australia
    - Industry develops rules
- Self-regulation
  - Code of practice/conduct

Adapted from Dr. Malin's slides.

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
  - Applies 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

The Privacy Act of 1974, 5 U.S.C. § 552a.

Freedom Of Information Act (FOIA)

- Established in 1966 (most recently amended in 2016)
- 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

- State: Limited, usually concerned with embarrassing facts
- State constitutions:
  - California: “All people are by nature free and independent and have inalienable rights. Among these are…pursuing and obtaining safety, happiness, and privacy”
  - Hawaii: “The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest”

Financial Services Modernization Act of 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

http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

Children's Online Privacy Protection Act (COPPA) of 1998

- 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

http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Family Educational Right to Privacy (FERPA) of 1974

- 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

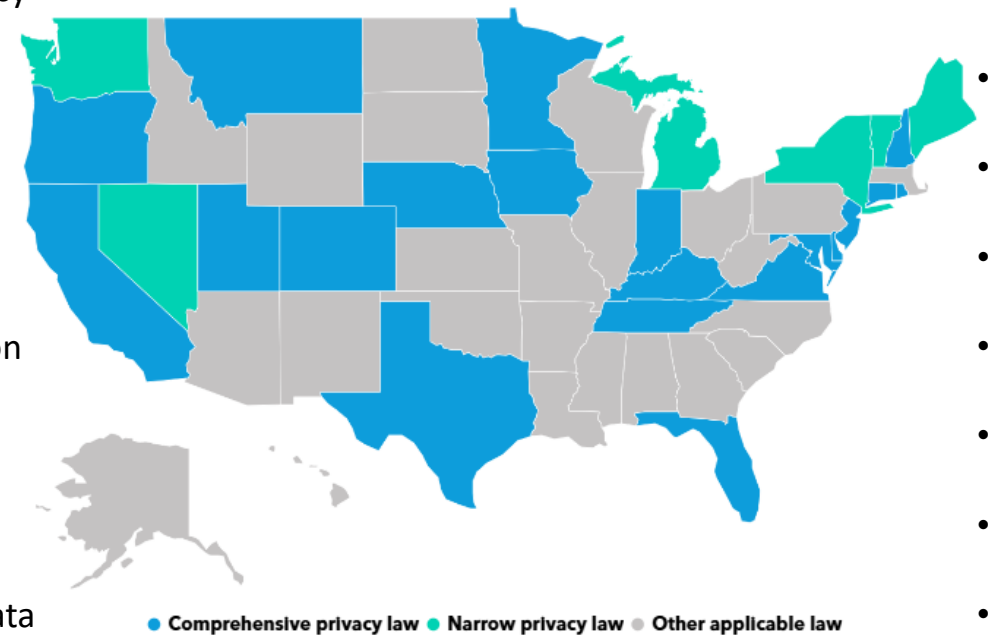
Family Educational Right to Privacy (FERPA) of 1974

- Schools may disclose, without consent, "directory" information, such as:
  - name
  - address
  - telephone number
  - date and place of birth
  - honors and awards
  - and dates of attendance
- Schools must notify parents and eligible students
  - about directory
  - allow request not to disclose
  - about FERPA rights annually

https://registrar.vanderbilt.edu/ferpa/

Twenty States Now Have Consumer Protection / Privacy Acts

- California: California Consumer Privacy Act (CCPA) and its amendment, California Privacy Rights Act (CPRA).
- Colorado: Colorado Privacy Act (CPA).
- Connecticut: Connecticut Data Privacy Act (CTDPA).
- Delaware: Delaware Personal Data Privacy Act.
- Florida: Florida Consumer Data Protection Act.
- Indiana: Indiana Consumer Data Protection Act.
- Iowa: Iowa Consumer Data Protection Act (Iowa CDPA).
- Kentucky: Kentucky Consumer Data Protection Act.
- Maryland: Maryland Consumer Data Protection Act.
- Minnesota: Minnesota Consumer Data Protection Act.



- Montana: Montana Consumer Data Privacy Act.
- Nebraska: Nebraska Consumer Data Protection Act.
- New Hampshire: New Hampshire Consumer Data Protection Act.
- New Jersey: New Jersey Consumer Data Protection Act.
- Oregon: Oregon Consumer Privacy Act (OCPA).
- Rhode Island: Rhode Island Consumer Data Protection Act.
- Tennessee: Tennessee Information Protection Act (TIPA).
- Texas: Texas Data Privacy and Security Act.
- Utah: Utah Consumer Privacy Act (UCPA).
- Virginia: Virginia Consumer Data Protection Act (VCDPA).

https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#states-with-comprehensive-data-privacy-laws [April 7, 2025]

California

- California Consumer Privacy Act (CCPA)
- California residents
  - Can ask businesses to disclose what personal information they have about you and what they do with that information
  - Can request business to delete your personal information
  - Can tell business not to sell your personal information
    - Businesses must wait at least 12 months before asking you to opt back into the sale of your personal information

California - Application

- Apply to businesses when they exceed one of the following:
  - Annual gross revenues of $25 million;
  - Annually buy, sell, receive, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
  - Derive 50 percent or more of its annual revenues from selling consumers' personal information.
  - Parent companies and subsidiaries sharing the same branding must also comply even if they themselves do not exceed the applicable thresholds.

California – Personal Information

- “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

- Statute includes a non-exhaustive list of 11 categories of data that fall under this definition
  - One of the categories is “biometric information”

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

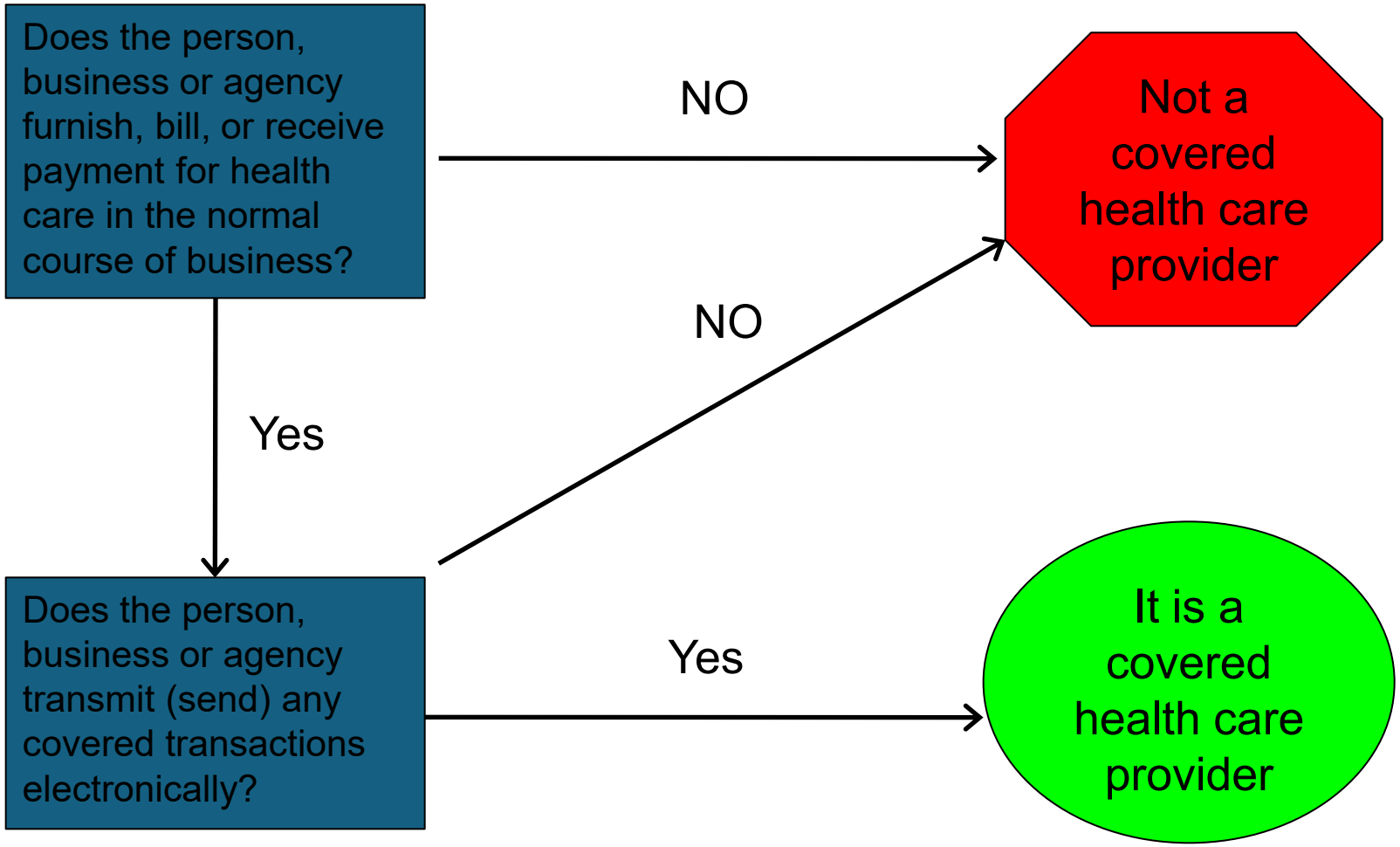
HIPAA Definitions

- 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

HIPAA Definitions

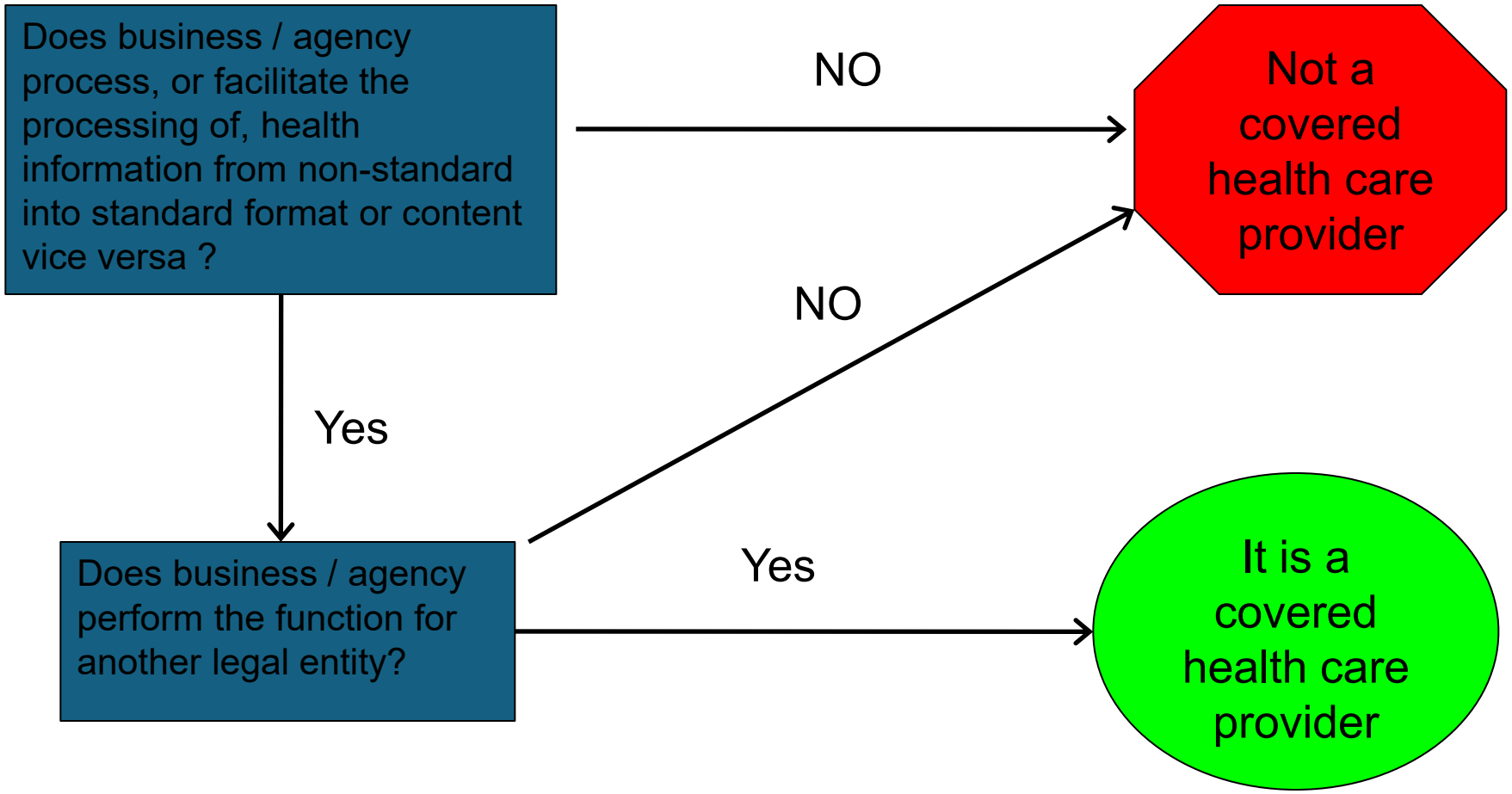
- Protected Health Information (PHI)
  - Individually identifiable health information
  - Identifiable corresponds to data that is “explicitly” linked to a particular individual
    - But also includes health information that includes data which could reasonably be expected allow individual identification

Covered Health Care Provider?



https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html

What is a Clearinghouse?



https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html

Examples of Covered Entities

- Health Plans
  - HMOs
  - Company health plans
  - Health maintenance companies
  - Medicare
  - Medicaid
  - Employers and schools who handle PHI when they enroll employees and students in health plans
- Health Care Clearinghouses
  - Billing services
  - Community health management information system
- Health Care Providers
  - Physicians
  - Surgeons
  - Dentists
  - Podiatrists
  - Laboratory technicians
  - Optometrists
  - Hospitals
  - Clinics
  - Nursing homes
  - Pharmacies
- Business Associates
  - Data transmission providers
  - Data processing firms
  - Data storage or document shredding companies
  - Medical equipment companies
  - Consultants hired for audits, coding reviews, etc.
  - Electronic health information exchanges
  - Medical transcription services
  - External auditors or accountants

https://www.forbes.com/sites/thesba/2014/02/06/does-your-business-need-to-be-hipaa-compliant/#615189973d7c

HIPAA – Data Protection

- PRIVACY RULE (2002)
  - Dept of Health & Human Services. Standards for privacy of individually identifiable health information; Final Rule. Federal Register. 45 CFR: Pt 160 and 164.

- SECURITY RULE (2003)
  - Dept of Health & Human Services. Standards for the Protection of Electronic Health Information; Final Rule. Federal Register. 45 CFR: Pt 164.

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)

- De-identified Data
  - Safe Harbor (A DIFFERENT ONE!)
  - Statistical or Scientific Standard
  - … note that State data protection regulations also have de-identification provisions!

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 (cont'd)

- Data that can be given away by a covered entity
- Requires removal of eighteen direct and other "quasi-"identifiers
  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 Harbor vs. Limited Data Sets

Less strict but limited sharing!

- 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

What about Research?

- HIPAA corresponds to information generated during healthcare
- Does this apply to information collected for research?

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.”

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

- National Institutes of Health. Final Statement on Sharing Research Data. NOT-OD-03-032. Feb 26, 2003.
  - http://grants.nih.gov/grants/guide/notice-files/not-od-03-032.html

- "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"

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

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

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

- 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

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

http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361 [2015]

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

Article 29 Working Party Opinion (April 2014)

- Do not rely on the “release and forget” approach.
  - Given residual risk of identification, data controllers should:
    - Identify 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

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

European Medicines Agency Steps In (October 2014)

- Promulgated 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”

http://www.ema.europa.eu/docs/en_GB/document_library/Other/2014/10/WC500174796.pdf

The General Data Protection Regulation (GDPR) of 2018

- Personal Data
  - Any information that relates to an identified or identifiable individual. It can be one item or a collection of items that, together, can identify an individual.
- Special categories of personal data
  - Items in this category may not directly reveal the identity of an individual, but instead they may indirectly confirm protected information
  - race, ethnicity or sexual orientation, political, religious or philosophical beliefs. Genetic or biometric data used to uniquely identify someone. Health information, union membership

Terms of Roles

- Data Subject
  - Any individual whose data is being collected and whose privacy rights are under the protection of GDPR
- Data Controller
  - Any organization in possession of personal data.
  - Data controllers determine how they will **store, process, use, transfer, and destroy** data.
- Data Processor
  - In the event a data controller does not do their own processing, they can employ a natural or legal person to **store, process, transmit, and destroy** personal data

Terms of Roles

- Data Protection Authority
  - Independent national public authority that protects its citizens and residents fundamental privacy rights.
  - E.g., German Federal Commissioner for Data Protection and the Croatian Personal Data Protection Agency.
- Data Protection Officer
  - a GDPR expert who ensures their organization is GDPR compliant.

Rights of data subjects

- **The right to be informed**
  - Subjects must be given explicit details about how their data will be used.
  - Data controllers must obtain permission to collect personal data from the subject themselves
- **The right of access**
  - Data controllers must be transparent with the data they process.
  - Data subjects have the right to access and view their data at any time.
  - They can see for themselves that it does not include any details they did not agree to share or that it does not contain inaccuracies.
  - Subjects can also request copies of their data free of charge.
  - Data controllers have a responsibility to inform subjects of the channels for which they can do this and they must maintain the integrity of those channels

Rights of data subjects

- **The right to rectification**
  - In the event a data subject reviews their data and finds inaccuracies, they have the right to request rectification
- **The right to object to processing**
  - In certain situations, controllers must stop processing personal data if a subject objects, this is true even if that subject had previously given their consent.
- **The right not to be subject to a decision based solely on automated processing**
  - simply offers a data subject a way to defend themselves against decisions made based on automated mechanisms that do not involve an actual human

- **The right to erasure (the right to be forgotten)**
  - Subjects have the right to have their personal data permanently erased from a data controllers database at any time
  - Controllers must also delete all copies of the individual's personal data that exists in all third party databases.
  - Exceptions (e.g., controllers have reasons of public interest, scientific or historical research, or statistical purposes)
- **The right to data portability**
  - Individuals have the right to ask the data controller to transmit a copy of their personal data to another controller.
  - The data must be in a structured, commonly used, and machine readable format.
  - It only applies to the data the subject themselves has provided to the controller.
- **The right to restrict processing**
  - A data subject has the right to request limit the ways in which controllers use their data

Take-away messages

- Know key concepts in HIPAA
  - Covered Entities
  - Protected health information (PHI)
  - Privacy Law – HIPAA Safe Harbor (18 identifiers to be removed)
- Know key concepts in GDPR
  - Five roles
  - Eight rights of data subjects, especially the right to be forgotten

Readings due on November 5

- 1. Sweeney L. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.
  - https://dataprivacylab.org/projects/identifiability/paper1.pdf
- Optional
  - ❑ Golle P. Revisiting the uniqueness of simple demographics in the US population. In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society 2006 Oct 30 (pp. 77-80).
    - ❑ https://crypto.stanford.edu/~pgolle/papers/census.pdf

Feedback Survey

- One thing you learned or felt was valuable from today's class & reading

- Muddiest point: what, if anything, feels unclear, confusing or "muddy"

- https://www.wjx.cn/vm/hX0mIro.aspx