Policies and Regulations

The good stuff is from Carole Palmer and Cheryl Thompson

Privacy

The laws

The data

The challenges

The remedies

and the bits that tell on you [what's on your hard disk (outside the filesystem)]

Privacy related policies

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- The Privacy Act of 1974
- The Freedom of Information Act (FOIA)
- Code of Federal Regulations on Protection of Human Subjects (Common Rule: 45 CFR 46; 21 CFR 56)
- Gramm-Leach-Bliley Act

What kinds of data are regulated?

Names

Geographic locations smaller than a state

Zip codes

Dates (e.g., birth, death, health care services)

Telephone numbers

Fax numbers

Email addresses

Social security numbers

Medical record numbers

Health plan beneficiary identifiers

Account numbers

Certificate/license numbers

Vehicle identifiers (e.g., license plate)

Device identifiers and serial numbers

Web universal resource locators (URL)

Internet protocol (IP) address numbers

Biometric identifiers, including finger and voice prints

Full face photographic images

Any others?

Challenges

Complying with regulations (e.g., HIPPAA, FERPA)

- Handling/protecting data with sensitive information
- Designing secure environments
- Establishing access rights

What does consent, privacy, and harm all mean in the digital world and social media?

HIPAA

HIPAA has several features

- Health insurance coverage for workers and their families
- Establishment of national standards for digital health care transactions
- Guidelines for pre-tax medical spending accounts and group health plans
- Governs company-owned life insurance policies

HIPAA Privacy Rule

"…establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures…" – From HHS.gov

HIPAA

- Personal health information (PHI)
  - "is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment."

- List of 18 identifiers
  1. Names;
  2. All geographical subdivisions smaller than a State,
  3. All elements of dates (except year) for dates directly related to an individual
  4. Phone numbers;
  5. Fax numbers;
  6. Electronic mail addresses;
  7. Social Security numbers;
  8. Medical record numbers;
  9. Health plan beneficiary numbers;
  10. Account numbers;
  11. Certificate/license numbers;
  12. Vehicle identifiers and serial numbers, including license plate numbers;
  13. Device identifiers and serial numbers;
  14. Web Universal Resource Locators (URLs);
  15. Internet Protocol (IP) address numbers;
  16. Biometric identifiers, including finger and voice prints;
  17. Full face photographic images and any comparable images; and
  18. Any other unique identifying number, characteristic, or code

Some privacy protection techniques

- Obtain consent from participants (ideal)
- Anonymization
  - Remove values
    - Focus on combination of variables
  - Redaction
  - Aggregations
  - Statistical disclosure control
    - Statistical Disclosure Control: This technique is most often used on aggregated data to modify individual observations to prevent identification. It can involve introducing random noise to continuously measured observations or aggregated statistics, randomly permuting responses, or suppressing aggregate results based on too few observations.

Anonymization example

ID	Original Response(s)	Changed to
123	01/31/1981	Age 30-40
456	Chicago, IL	US city
789	Cheryl (real name)	Bess (pseudonym)
122	Chief Data Officer	Senior executive
155	UIUC	State university
156	Female, 37, Caucasian	Male, 40, Caucasian
814	Female, 61821, 40, Blue	, , , Blue

Additional Resources

- Data-PASS confidentiality policies. http://www.data-pass.org/sites/default/files/confidentiality.pdf
- Qualitative Data Archive. A Guide to Sharing Qualitative Data. https://qdr.syr.edu/guidance/sharingdata

BitCurator Access

- BitCurator has developed set of digital forsenic tools for digital materials
- works below the file system, at the block level),
- Tools for identifying and redacting sensitive information:
  - Email address
  - Geolocation metadata
  - Credit card numbers
  - SSNs

https://www.bitcurator.net/

Readings

Required:

Browse: "List of Federal Agency Public Access plans." http://bit.ly/FedOASummary

Stodden, V. (2009). The Legal Framework for Reproducible Scientific Research: Licensing and Copyright. *Computing in Science & Engineering,* 11(1): 35-40. http://dx.doi.org/10.1109/MCSE.2009.19

Carroll, M.W. (2015). Sharing Research Data and Intellectual Property Law: A Primer. *PLoS Biology*, 13(8): e1002235. http://doi.org/10.1371/journal.pbio.1002235

Fact Sheet on the Illinois Open Access to Research Articles Act (Public Act 098-0295). https://publish.illinois.edu/commonsknowledge/2013/08/22/fact-sheet-on-the-illinois-open-access-to-research-articles-act-public-act-098-0295/

For Review:

Tanner, A. (2013). Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study. *Forbes.* http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#727260933e39

Abowd, J. M., Vilhuber, L., & Block, W. (2012). A proposed solution to the archiving and curation of confidential scientific inputs. In J. Domingo-Ferrer & I. Tinnirello (Eds.), *Privacy in Statistical Databases* (pp. 216-225). Berlin Heidelberg: Springer.

Policies (take a look)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Family Educational Rights and Privacy Act (FERPA)
The Privacy Act of 1974
The Freedom of Information Act (FOIA))
Code of Federal Regulations on Protection of Human Subjects (Common Rule: 45 CFR 46; 21 CFR 56)
Gramm-Leach-Bliley Act