Data Lifecycle: Planning

CSCI 220: Database Management and Systems Design

Based on the University of Wisconsin-Madison's
Data Literacy Training Materials

U.S. Fish and Wild Life Service's Data Lifecycle

https://www.fws.gov/data/life-cycle

Why Not “Move Fast and Break Things?”

- Planning saves time in the long run
- Planning helps you recover from disasters (hackers, hardware failure, etc.)
- Avoid lawsuits by following laws governing use of people’s data

Data Management Plan: Basics

- What data do you collect?
- Where does your data come from?
- Why are you collecting the data?

Data Management Plan: Other Concerns

- Who is responsible for technical aspects of your data? Legal aspects?
- When can/should the data be deleted (retention)?
- Can you attribute changes to the data (auditability)?
- Will the data be shared with other organizations?
- How to keep the data management plan up-to-date?

Data-Related Laws and Regulations

- A (very) incomplete list:
  - GDPR: General Data Protection Regulation
  - CCPA: California Consumer Privacy Act
  - COPPA: Children’s Online Privacy Protection Rule
  - HIPPA: Heath Insurance Portability and Accountability Act
  - PCI-DSS: Payment Card Industry Data Security Standard

GDPR: General Data Protection Regulation

- European Union law which governs processing of individuals' data
- "The GDPR has a chapter on the rights of data subjects (individuals) which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing."
- Applies to US companies which process EU residents' data

https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en

CCPA: California Consumer Privacy Act

- “This landmark law secures new privacy rights for California consumers, including:
  - The **right to know** about the personal information a business collects about them and how it is used and shared;
  - The **right to delete** personal information collected from them (with some exceptions);
  - The right to **opt-out** of the sale or sharing of their personal information;
  - …”

https://oag.ca.gov/privacy/ccpa

COPPA: Children's Online Privacy Protection Rule

- "The Rule applies to operators of … online services … **directed to children** under 13 that collect, use, or disclose personal information from children … **[and]** to operators of … online services **with actual knowledge** that they are collecting, using, or disclosing personal information **from children** under 13… Operators covered by the Rule must:
  - Post a clear and comprehensive online privacy policy describing their information practices…
  - …obtain verifiable parental consent … before collecting personal information … from children
  - Give parents the choice of … prohibiting [information disclosure] to third parties…
  - Provide parents access to their child's personal information to review and/or [delete]
  - Maintain the confidentiality, security, and integrity of information they collect from children
  - …"

https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

HIPPA: Heath Insurance Portability and Accountability Act

- Regulates health plans and most healthcare providers
  - **Doesn't** regulate life insurers, employers, most apps, …
- "Your health information cannot be used or shared without your written permission unless this law allows it."
- Gives individuals rights to access and correct health records

https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

PCI-DSS: Payment Card Industry Data Security Standard

- Credit card companies won't allow you to process customers' credit card information unless you adhere to PCI-DSS
  - Internal or external certification of compliance
- 300+ page document outlining security requirements. For example:
  - "Live [credit card numbers] cannot be present in pre-production environments outside the [cardholder data environments]."

https://www.pcisecuritystandards.org/document_library/

Data Breach Laws

- “All states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.”

- MA Data Breach Notification Law:

  - Requires notification of the state government and of consumers

  - Only applies to SSN, driver’s license, or financial account numbers

https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

https://www.mass.gov/info-details/requirements-for-data-breach-notifications

M UNIVERSITY OF MICHIGAN

PO Box 480149
Niles, IL 60714

October 23, 2023

Dear Peter Story,

On behalf of the University of Michigan, we are writing to inform you about an incident that involved personal information about you. Protecting the information entrusted to the University of Michigan is a responsibility that we take seriously, and we apologize that this incident occurred.

WHAT HAPPENED. On August 23, 2023, the University detected suspicious activity on the University of Michigan campus computer network. We took quick and decisive action to contain the incident, including proactively disconnecting the campus network from the internet. We quickly launched an investigation with the support of leading third-party experts. Based on our investigation, we have determined that an unauthorized third party was able to access certain University systems from August 23, 2023 to August 27, 2023.

WHAT INFORMATION WAS INVOLVED. The University used a dedicated review team to conduct a detailed analysis of the files included on the systems accessed by the unauthorized actor. Based on this data analysis, we believe that the unauthorized third party was able to access personal information relating to certain students and applicants, alumni and donors, employees and contractors, University Health Service and School of Dentistry patients, and research study participants. The following provides examples of the types of information, in addition to an individual's name, that may have been accessed, depending on an individual's affiliation with the University.

Students, applicants, alumni, donors, employees, and contractors: Social Security number, driver's license or other government-issued ID number, financial account or payment card number, and/or health information.

Research study participants and University Health Service and School of Dentistry patients: Demographic information (*e.g.*, Social Security number, driver's license or government-issued ID number), financial information (*e.g.*, financial account or payment card number or health insurance information), University Health Service and School of Dentistry clinical information (*e.g.*, medical record number or diagnosis or treatment or medication history), and/or information related to participation in certain research studies.

Review of Regulations

- If you collect users' data, you have legal obligations
- Collecting users' data is risky! Consider:
  - Storing all data on users' own devices
  - Encrypting users' data before you receive it (and keeping the encryption key exclusively on users' devices)
- In general, **documentation is essential** for compliance (ER models, etc.)!

Example: Satisfying “Right to Erasure”

- How to adhere to GDRP and CCPA’s “right to erasure?”
- A (properly implemented) relational database makes this easy!
  - Model a user as an entity. The user’s data will be attributes of that entity, or have relationships with that entity.
  - When a user instance is deleted, related records can be deleted by the database automatically: **a cascading delete**