# Privacy and the University of Oregon

**Mary Kay Fullenkamp, HIPAA and Privacy Officer**

**Ken Kato, Director GIS and Mapping**

UNIVERSITY OF OREGON

Safety and Risk Services

# Privacy by Design

"The philosophy and approach of embedding privacy into the design, operation, and management of IT and systems across the entire information life cycle.

***It is not bolted on as an add-on.***

The result is that privacy becomes an essential component of the core functionality being delivered."

*-Ann Cavoukian*

*Former Information and Privacy Commissioner*

*Ontario, Canada*

# Today’s Discussion

- Privacy considerations
- Fair Information Practices
- Privacy by Design – Examples of Success!

# What does Privacy include?

- For what purpose(s) are you collecting the data?
- How much do you need to collect for the intended purpose?
- Who can access the data?
- With whom will you be sharing the data?
- How long will you retain the data?

# Primary regulatory considerations


**HIPAA:** Intended to give the patient/client control over their information while allowing the flow of information necessary to deliver services.


**FERPA:** Intended to protect the privacy interests of students in their education records.


**Oregon Consumer Identity Theft Protection Act:** Ensures the notification of a consumer whose identity has been compromised.


**Federal Trade Commission:** Regulatory agency concerned with unfair or deceptive data privacy and security practices that put consumer's personal data at unreasonable risk.

**EU General Data Protection Regulation:** Applies to the Processing of personal data of an individual located in the EU, where the processing activities are related to the offering of goods or services.

# *RISKS* to the University

- Average published HIPAA fine amount in 2018 was approximately $2.8 million. Fines usually accompany a Resolution Agreement lasting 3-5 years. Stringent breach notification requirements exist.
- Penalties for non-compliance with FERPA range from a cease and desist letter to withholding of DOE payments.
- Consequences for violations of Oregon Consumer Identity Theft Protection Act include notification of individual, State Attorney General, and civil penalties up to $20,000 per offense.
- FTC fines can be onerous. An extreme example is the $22 million fine for Google in 2012. Facebook received a 20 year monitoring agreement in 2012.
- EU GDPR fines can reach 20,000,000 Euros or 4% of an organization or company's annual turnover. Data breach notification requirements exist.

# Value of Reputational Harm?

- **Portland State University Researchers May Have Violated Federal Law by Using the Personal Data of Thousands of Portland Area K-12 Students**. The University has since acknowledged it failed to inform parents of the research and did not get their permission to access the student data.
- **Stanford University privacy breach involves the data of 20,000 emergency room patients**. Information breached included, diagnoses, treatment, billing information, and discharge dates.

# Fair Information Practices

- *Fundamental set of core principles* and practices intended to provide guidance about data collection, handling, management and sharing in the interest of safeguarding privacy.

- Set forth by the *Office for Economic Cooperation and Development*.

- Many *U.S. laws* are modeled after these principles in addition to *international privacy agreements, codes, or recommendations*.

# Fair Information Practices

## Openness and Transparency

- Information about the policies and practices related to sharing personal information should be readily available

## Purpose Specification

- The purpose for which the data is collected should be clearly communicated at the time of collection

## Collection Limitation

- The data collected should be lawful and limited to the amount needed for the purpose specified.

## Data Minimization

- Collection of personally identifiable information should be kept to a strict minimum.

## Individual Participation

- An individual should have the right to access the data, make corrections, request erasure, and challenge the accuracy of the data.

## Data Quality

- The integrity of the personal data should be protected against alteration or modification.

## Security Safeguards

- Personal data should be protected by reasonable security safeguards against unauthorized access destruction, and inappropriate use.

## Accountability

- A processor or holder of the data should be accountable for measures to support these principles.

# Stress Neurobiology and Prevention Lab (SNAP)

- Implements a video coaching program for caregivers of young children that focuses on developmentally supportive interactions.
- Videos of caregiver-child interactions are shared between the SNAP Lab and community-based organizations for use in services and support.

# SNAP Lab

- Collect only the amount of information necessary to provide the services.  Do not receive a client record.
- Review of consent process.
- Examine any sharing of information and why.
- Security review conducted for transfer, storage, and sharing of films.
- Participant families have the option to access and obtain a copy of the film.
- Privacy training conducted for lab staff and students.
- Assessment conducted of work space for privacy and security concerns.

# Resources for Privacy Consultation

- Privacy Office
- Office of General Counsel
- Information Services
- Innovation Partnership Services
- Sponsored Project Services
- Purchasing and Contract Services

# Thanks for your attendance!

marykayf@uoregon.edu

541-346-2513