Safeguarding the privacy and confidentiality of individuals’

Nahnsan Guseh, SUMR Scholar 2018

Overview

Privacy is an important part of our lives. Information of ourselves can be used in many ways to make things personalized for you, marketing/advertising purposes or to take advantage of people

Rapid technology brings opportunities to improve health

Challenges arise

Aim

Understand the risks to privacy and how the US can guard against them while taking full advantage of accelerating progress in health technology

What is HIPAA

The Health Insurance Portability & Accountability Act - 1996

- The law restricts access to individuals' private medical information
- Its Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits on the uses and disclosures that may be made of information without patient authorization.
- The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronically shared and stored personal health information.
- Outdated

HIPAA applies only to "covered entities" — defined as health plans, health care clearinghouses, and health care providers who transmit health information electronically

- Also to "business associates," including individuals and companies, such as IT support firms, that help covered entities handle their electronic information

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

HHS

What is not a covered entity

You tell your doctor to give part of your health records to your employer to explain your absence from work. The record will probably not be subject to HIPAA in the hands of your employer.

A health researcher obtains your health records for use in a properly authorized research project. The records have no HIPAA protection in the hands of the researcher -- unless it is a clinical trial.

Businesses that do not directly engage in the provision of health care or health insurance including Apple, Fitbit and other similar companies that make/sell wearable devices that collect and share health data.

Selected Privacy and Security Safeguards.	
Type of Safeguard	**Examples**
Physical	
Confidential patient care	Private examination and consultation rooms; conducting phone calls and other conversations where unlikely to be overheard; attention to eavesdropping risks
Document storage	Secure-access filing for medical records and bills; controlled prescription pads
Document disposal and destruction	Shredding
Electronic	
User authentication	Passwords; biometric identification; automatic logouts
Systems protections	Firewalls; antivirus programming; active audit trails
Safe hardware disposal	Erasing hard drives from rented photocopiers; proper disposal of used computers
Human capital	
Careful hiring practices	Careful vetting of potential hires, including the use of background checks
Training and education	Education about individually identifiable information; appropriate information sharing; protocols for screening information seekers
Termination and separation protocols	Timely deactivation of electronic and physical access

GDPR

General Data Protection Regulation

- GDPR standardizes data protection across the EU
- It just took effect … May 2018
- New, stricter rules on how companies must handle and protect individuals' personal data
- GDPR's goal is to give users more control over and clarity of their information
- Forces companies to explain/justify what they do with your data.
- Any organization/business that holds personal data is expected to comply
- GDPR applies to EU companies and to others, wherever located, that do business in the EU

What is Personal Data

Under GDPR -- Anything that can identify you. I.E name, phone number, username, location/ip, health data, political opinions, sexual orientation & etc..

Wearable Devices

Technology that is worn on the human body, including powerful sensor technologies that can collect and deliver information about users & their surroundings.

Apple Watch, Fitbit, Actigraph & other smartwatches and fitness trackers

- Location data
- Heart rate
- Steps
- Sleep patterns
- & Much More

Genetic Privacy

- Privacy Policies - Wordy, difficult to read and understand
- Accelerate process of a more transparent privacy policy with users

  Genetic Testing Companies such as ***23andMe***, ***Ancestry/DNA*** & other similar sites

- Standardization of privacy policies

ISSUES		QUESTIONS
A. Information Collection:	1	Do they have the privacy policy on their website?
	2	Do they require consumers to actively consent to the privacy policy?
	3	Do they collect information from outside sources (not just directly from consumers)?
	4	Do they use cookies and similar tracking technologies?
	5	Do they allow third parties to use cookies and similar tracking technologies?
	6	Do they collect registration information?
	7	Do they collect genetic information? (AWO added)
	8	Do they collect other sensitive information? (AWO added)
	9	What else do they collect? (NG added)
	10	Do they give users choices over the use of their information? (NG added)
	11	Do they list their related brands? (NG added)
B. Information Processing:	1	Do they de-identify the data before sharing outside the organization?
	2	Do they encrypt the data (e.g., do they hashtag passwords)?
	3	Do they protect against re-identification?
	4	Do they save your DNA sample?
	5	Do they store the data in secure rooms?
	6	Do they use the data for research?
	7	Do they conduct third-party security audits?
	8	Do they list their research partners? (NG added)
	9	Do they discuss how they'll handle privacy policy changes? (AR added)
	10	Do they reference EU protections?
	11	Do they explain the process/timing by which you can revoke consent to keep DNA data?

C. Information Dissemination	1	Do consumers own their data?
	2	Do consumers have the right to access their data?
	3	Do consumers have the right to delete their data, except for ongoing research?
	4	Do they share the data with service providers?
	5	Do they share the data with other outside entities or persons?
	6	Do they use sensitive (e.g., genetic) information for advertising?
	7	Do they have the right to sell the data?
	8	Do they restrict which employees have access to the data?
	9	Do they allow law enforcement to access the data?
	10	Do they educate/advise about privacy and other concerns?
	11	Do they allow the user to share information with outside parties?
	12	How well do they handle the sharing decisions that the user makes? (NG added)
D. Invasion:	1	Do they protect against employers' and insurers' access to sensitive information?
	2	Do they have explicit procedures for a data breach?
	3	Do they expressly promise to notify users in event of a data breach?
E. General:	1	Readability, understandability, user-friendliness? (AJR added)

What's Next

Continue to add to document

Meet with HHS (Oct.22 symposium in DC focus on health information privacy)

Suggest a Privacy Policy Standardization and consider the best entity(ies), gov't or otherwise, to implement and enforce the new guidelines.

Other Project - Medicaid Expansion

Comparing medicaid expansion to housing market growth

- Urban Economics Theory

- Is the Housing market affected

	Alabama	Alaska	Arizona	Arkansas	California	Colorado	Conneticut	Delaware	Florida
Mar-17	N	E	W	E	E	E	E	E	N
Apr-17	N	E	W	E	E	E	E	E	N
May-17	N	E	W	E	E	E	E	E	N
Jun-17	N	E	W	E	E	E	E	E	N
Jul-17	N	E	W	E	E	E	E	E	N
Aug-17	N	E	W	E	E	E	E	E	N
Sep-17	N	E	W	E	E	E	E	E	N
Oct-17	N	E	W	E	E	E	E	E	N
Nov-17	N	E	W	E	E	E	E	E	N
Dec-17	N	E	W	E	E	E	E	E	N
Jan-18	N	E	W	E	E	E	E	E	N
Feb-18	N	E	W	E	E	E	E	E	N
Mar-18	N	E	W	E	E	E	E	E	N
Apr-18	N	E	W	E	E	E	E	E	N
May-18	N	E	W	E	E	E	E	E	N
Jun-18	N	E	W	W	E	E	E	E	N
Jul-18	N	E	W	W	E	E	E	E	N
Aug-18	N	E	W	W	E	E	E	E	N

KEY		
	N	Has not expanded Medicaid
	E	Medicaid Expansion Implemented under the ACA
	W	Medicaid Expansion Implemented under the ACA With Waiver Approved & using Waiver
	WW	Had existing waiver, but waiver was edited

AS OF AUG-1-2018	
Number of states that fully expanded medicaid	25
Number of states that expanded w/ a waiver	5
Number of states that did not expand medicaid at all	19
Number of states with a newly changed waiver	1
TOTAL	50

Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates

Insurers & data brokers are working together

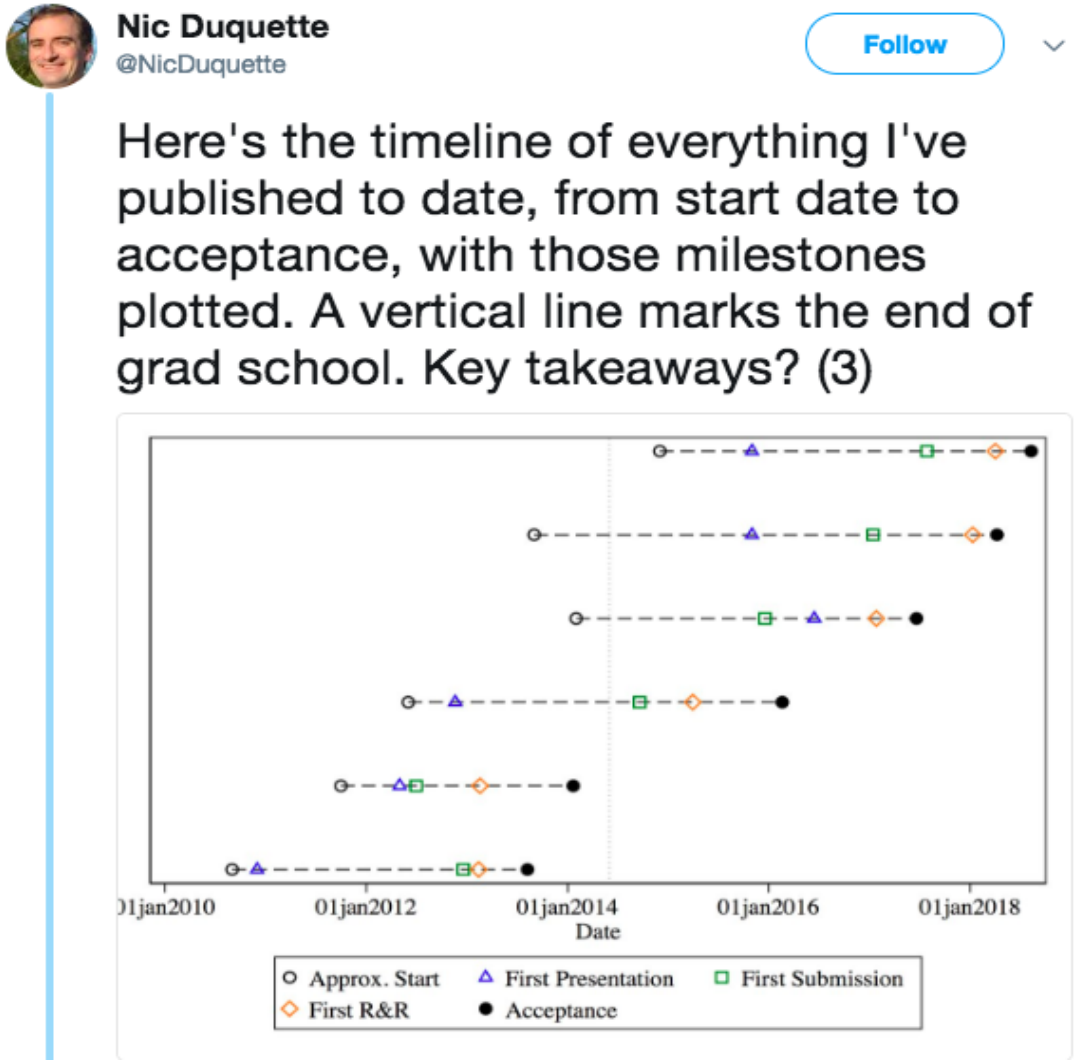
Possible implication -- Where everything you do, the things you buy, the food you eat, the time you spend watching TV, will determine how much you pay for health insurance.

For example : Are you a woman who recently changed your name? You could be newly married and have a pricey pregnancy pending. Or maybe you’re stressed and anxious from a recent divorce.

This computer model may run up your medical bills.

Lessons Learned

- Research is slow -- Patience
- I love research



Thank You!