WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Health Data Privacy

Privacy Week Webinar
January 26, 2023

Presenter Introductions

Katy Ruckle
Washington State Chief Privacy Officer
WaTech

Jennifer Lee
Technology and Liberty Manager
American Civil Liberties Union of Washington

Overview of Material to Cover Today

- What are the concerns about health data privacy?
- What are the regulation approaches?
- What is the federal government doing?
- What are we doing in Washington?
- What are steps you can consider for your privacy?
- Additional information & Resources

O P D P

Isn’t my health data protected by HIPAA?

HIPAA = Health Insurance Portability and Protection Act – Federal law adopted in 1996

Short answer is “NO” HIPAA does not protect your health data in all cases.

But before we get to that let’s talk about what HIPAA does protect.

HIPAA boiled down:

- Privacy Rule – Keep PHI* private!
- Security Rule – Keep PHI secure!
- Breach Notification Rule – If you don't keep PHI private and secure you have to notify of a breach!

*PHI = "Protected Health Information" and is a defined term

Privacy Rule

Regulates the circumstances under which covered entities may use and disclose PHI and requires covered entities to have safeguards in place to protect the privacy of the information.

Examples of private client information include:

- Demographic (name, address, DOB, SSN, Driver's Lic #)
- Financial (credit card/bank acct #, claims info)
- Eligibility (client status; receiving public assistance)
- PHI (includes the above & clinical info – diagnosis, medications, lab results)

Security Rule

Requires covered entities to implement certain administrative, physical, and technical safeguards to protect electronic information.

Examples:

- Administrative Safeguard – training
- Physical Safeguard – key card access
- Technical Safeguard – encryption

Breach Notification Rule

Requires covered entities and Business Associates (contractors) to provide notification following discovery of a breach of unsecured protected health information.

"Unsecured PHI" is PHI that has not been made unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology such as encryption.

What is a Covered Entity?

The HIPAA Rules apply to **covered entities**, and to their business associates who perform functions or provide services for the covered entity.

A covered entity is a

- **health plan**,
- **health care provider**, or a
- **health care clearinghouse**

What is a Covered Entity?

- Health Plans (e.g. Medicaid)

- Health care providers are covered by HIPAA if they transmit **electronic** health information in connection with certain transactions, such as billing and payment.

- Health care clearinghouse (e.g. medical claims or 3rd party billing intermediary)

Note: Business Associates – contractors of covered entities who process PHI on covered entities behalf

Significant Consequences for Failure to Comply

As of 12/31/22 Feds settled or imposed penalties totaling **$133,578,772.00.**

Other regulations for Treatment of Health Data in Washington

- Uniform Health Care Information Act – RCW 70.02
- Ethics Law applicable to State Employees – RCW 42.52
- 42 CFR Part 2 – Substance Use Disorder Information

Serious consequences and liability for state employees

Ethical considerations for handling confidential information:

RCW 42.52.050:

Confidential information

(3) No state officer or state employee may disclose confidential information to any person not entitled or authorized to receive the information.

Chapter 42.52 is the Ethics in Public Service law

- Former employee (a nurse practitioner) posted photo of client to SnapChat
- Terminated from position
- Investigated by DOH and conduct was reported to National Practitioner Database and posted on DOH website
- Fined $2,000 by the Executive Ethics Board

HIPAA does not protect all health information

- Health information collected by apps that are not part of a covered entity or business associate are not subject to HIPAA.
- For example:
  - Fitness devices/wearables
  - Mobile fitness tracking apps
  - Sleep and heartrate monitors
  - Period tracking apps
  - Glucose pumps
- Health services provided by provider that does not electronically bill

Data Invasive Examples

Data Invasive Practices – Cell Phones

- According to a 2019 Vice Motherboard investigation, major mobile device service providers have sold customers' locations and PII to third-party companies, with the information eventually falling into the hands of bail bonds firms and bounty hunters.

- Cell phone information and online search results were used in the prosecution of a woman who experienced a pregnancy loss after searching online for medication abortion information.

Data Invasive Practices – Social media & Messaging Apps

- A teenager and her mother were indicted in the summer of 2022 in Nebraska. The mother's charges included violating the state's law banning abortion. In investigating the case, law enforcement obtained information from the daughter's social media messaging app.
- According to reports, the social media company shared the information with law enforcement in response to a judicial warrant that did not mention abortion.
- People who use social media and messaging apps can find themselves at risk when companies are allowed to retain and access private conversations between individuals.

Data Invasive Practices – Patients in waiting rooms - geolocation

- Patients waiting for emergency room medical care in Philadelphia were targeted with ads for personal injury lawyers, according to a 2018 NPR article.

- Geolocation data was used to target visitors to 140 abortion clinics with ads for anti-abortion pregnancy counseling services.

- In states where a miscarriage could result in a criminal investigation, geolocation data could carry risks that go far beyond unwanted advertising.

Data Invasive Practices – Patients in waiting rooms - geolocation

- A location data broker, sold location data of people who visited abortion clinics, including more than 600 Planned Parenthoods over a one-week period for $160.
- The data showed where patients traveled from, how much time they spent at the healthcare centers, and where they went afterwards.
- The data included an analysis of where people appeared to live, based on where their cell phones are commonly located overnight.

Data Invasive Practices – Health Apps

- Flo Health, one of the most popular period tracking apps, settled with the FTC over allegations that it shared health information on its 100 million users with third-party data analytics firms
- Even though users' location is not needed to use the app, individuals who use the MyDays cycle tracking app are continually having their location tracked,
- Users of MyDays location and personal information is then shared with a company that markets users' personal life details like "User has arrived at a clinic" or "User might be unfit to drive due to sleep deprivation" to insurance companies and other 3rd parties.

Data Invasive Practices – Health Information on Dating Apps

- Popular dating apps shared users' location and information intimate sexual information, alcohol use, ethnicity, age, and partner preferences with third parties
- Another dating app was sharing its users' HIV status and other PII with third parties.
- By comparison same information with HIPAA Protection: – Health Care insurer's mailing to customers made HIV status visible through envelope window. Company had to pay $1 million in HIPAA penalties and an additional $17 million to settle the lawsuits for the breach

Trends in Legislation

Health Privacy Legislation

Trends in bills include:

- Consumer data protections
- Data collection restrictions on apps
- Geofencing
- Limit on judicial orders
- Limit on subpoena/warrant response
- Limits on data brokers
- Internet search history protection
- Protections for providers/others

Proposed Federal Laws

- My Body May Data Act
- The 4th Amendment is not For Sale

Proposed Federal Laws

- My Body My Data Act
  - Limits data collection
  - Protects health data not protected by HIPAA (e.g. apps, cell phones and search engines)
  - Require privacy policy
  - FTC enforcement
  - Private Right of Action
  - Individual Rights/Consumer Protection for data access/deletion
  - Non-preemption for states with more restrictive laws

Proposed Federal Laws

The 4th Amendment is not For Sale

- Requires the government to get a court order to compel data brokers to disclose data
- Stops law enforcement from buying data on people
- Extends existing privacy laws to infrastructure firms that own data cables & cell towers.
- Closes loopholes permit gov't to buy metadata about Americans' international communication w/o FISA review
- Requires FISA rules for location data, web browsing, search histories

Legislation in Washington

- HB 1155 & SB 5531 “My Health My Data”
- Request legislation by the AGO
- Requires that any entity subject to the law must:
  - (1) Create and maintain a privacy policy specific to consumer health data;
  - (2) Provide consumers the right to request that the entity delete their health data;
  - (3) Requires opt-in consent for collection and sharing of consumer health data; and
  - (4) Fully prohibit the sale of consumer health data to third parties.

Legislation in Washington

Shield Law - House Bill 1469 and Senate Bill 5489

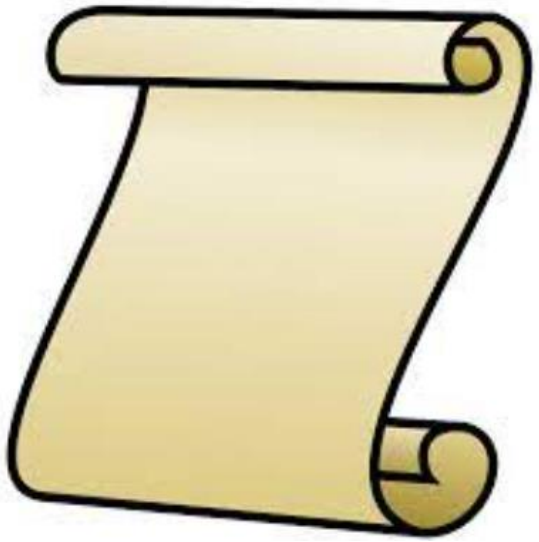
- Prohibit the issuance of out-of-state subpoenas seeking information related to abortion & reproductive health care services.
- Prohibit out-of-state criminal investigations & arrests seeking communication and other evidence related to abortion & reproductive health care services.
- Prohibit the Governor from extraditing any person for out-of-state charges regarding reproductive health care services.
- Provide a cause of action to recoup damages and other legal costs for hostile out-of-state lawsuits related to reproductive health care services.
- Protect health care service providers from harassment for providing protected health care services

Proposed WA Constitutional Amendment

HJR 4201 & SJR 8202

Governor proposed constitutional amendment for protection of reproductive rights

*This article is intended to expressly set forth the existing constitutional right to make reproductive freedom decisions for oneself included in a person's liberty, **privacy**, and equal protection rights guaranteed…*



Consumer Privacy Considerations

Steps you can take to protect your privacy with new health apps

- **Before downloading new app…**

✓**Use official app stores**

- Download apps only from official app stores, such as your device's manufacturer or operating system app store.

✓**Know what information the app will be able to access.**

- Read the app's privacy policy to see how your data will be used or if your data will be shared.
- Beware of vague policies about how the app will share your data.

Steps you can take to protect your privacy with new health apps

- ✓ **Check out the permissions.**
  - To gain access to information like your location or contacts or to get access to features like your camera and microphone, apps need your permission.
  - You may be asked to give permission when you first download the app, or at the time the app first tries to access that information or feature.
  - Pay close attention to the permissions the app requests.

Steps you can take to protect your privacy with apps you already use

✓ **Review the app's permissions.**

- Go to your settings to review the permissions to make sure the app doesn't have access to information or features it doesn't need.
- Turn off unnecessary permissions.
- Consider deleting apps that need a lot of permissions – some apps request lots of permissions that aren't needed for the app's function.
- Pay special attention to apps that have access to your contact list, camera, storage, location, and microphone.

Steps you can take to protect your privacy with apps you already use

- ✓ **Limit location permissions.**
  - Some apps have access to your device's location services. If an app needs access to your location data to function, consider limiting the access to only when the app is in use.
- ✓ **Keep apps updated.**
  - Apps with out-of-date software may be at risk of being hacked. Protect your device from malware by installing app updates as soon as they're released.

Steps you can take to protect your privacy with apps you already use

- ✓ **Don’t automatically sign-in to apps with a social network account.** Signing into an app with your social network account information often lets the app collect information from your social network account and vice versa. If you aren’t OK with that, use your email address and a unique password to sign in.

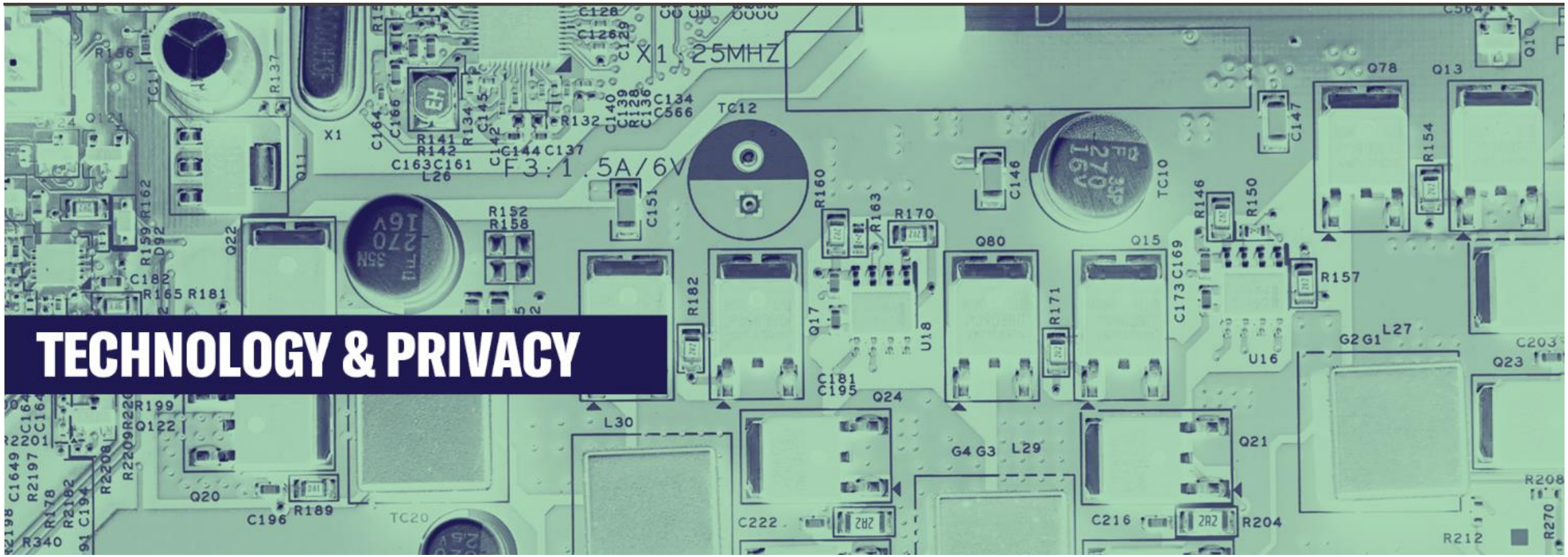
- ✓ **Delete apps you don’t need or no longer use.** To avoid unnecessary data collection, if you’re not using an app, delete it.

Additional Information & Resources

www.watech.wa.gov/privacy

OPDP

ACLU Technology and Liberty Project



Federal Trade Commission and Attorney General Office

https://www.ftc.gov/

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Identity Theft Awareness Week

From Jan. 30 to Feb. 3 the FTC and our partners will host free podcasts, webinars, Facebook Live interviews, and other events focused on avoiding and recovering from identity theft.

Visit identitytheft.gov to learn more.

https://www.atg.wa.gov/

Washington State
Office of the Attorney General
Attorney General
Bob Ferguson

- Consumer Protection Division
- File Consumer Complaints
- Warnings about Consumer Scams

Thank you!