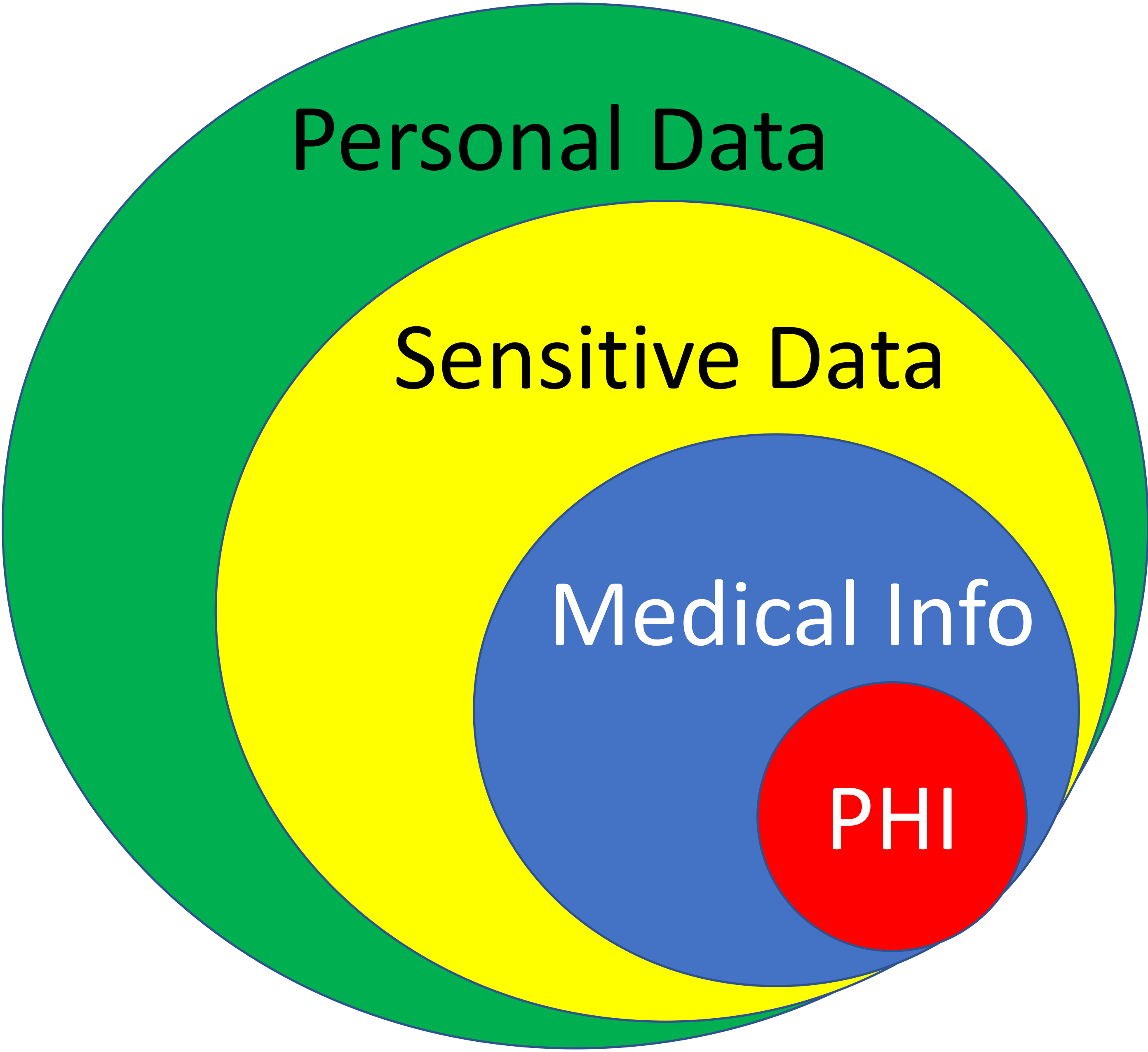
Emerging Issues in Digital Health Privacy



Hintze Law
Privacy + Data Security

Mason Fitch

Mason Fitch is an associate in Hintze Law's Health and Biotech Privacy Group. He is based out of Hintze Law's Houston office.

Mason counsels clients on a wide range of privacy and data security issues, particularly on privacy by design, data protection impact assessments, privacy policies, and development of privacy programs. Mason has experience with the HIPAA Privacy and Security Rules, state-based health information laws such as the California Confidentiality of Medical Information Act (CMIA), California Consumer Protection Act (CCPA), EU GDPR, biometric information privacy laws, FTC Act, development of internal privacy practices, M&A diligence, and online advertising.

Mason has significant experience in-house, both in legal and program management contexts. He was the first privacy hire at Hims & Hers Health, where he was responsible for all legal issues relating to privacy and security as well as the development of a privacy program. Prior to Hims & Hers Health, Mason was a Manager on the Privacy Program team at Meta (formerly Facebook). His team was responsible for conducting privacy reviews for all new or different uses of user data across Meta's messaging platforms, including Messenger, WhatsApp, and Instagram Direct. He launched the privacy review process at WhatsApp.

Mason started his legal career as an Associate at Debevoise & Plimpton LLP, where he counseled clients on GDPR compliance and participated in several high-profile white collar investigations.

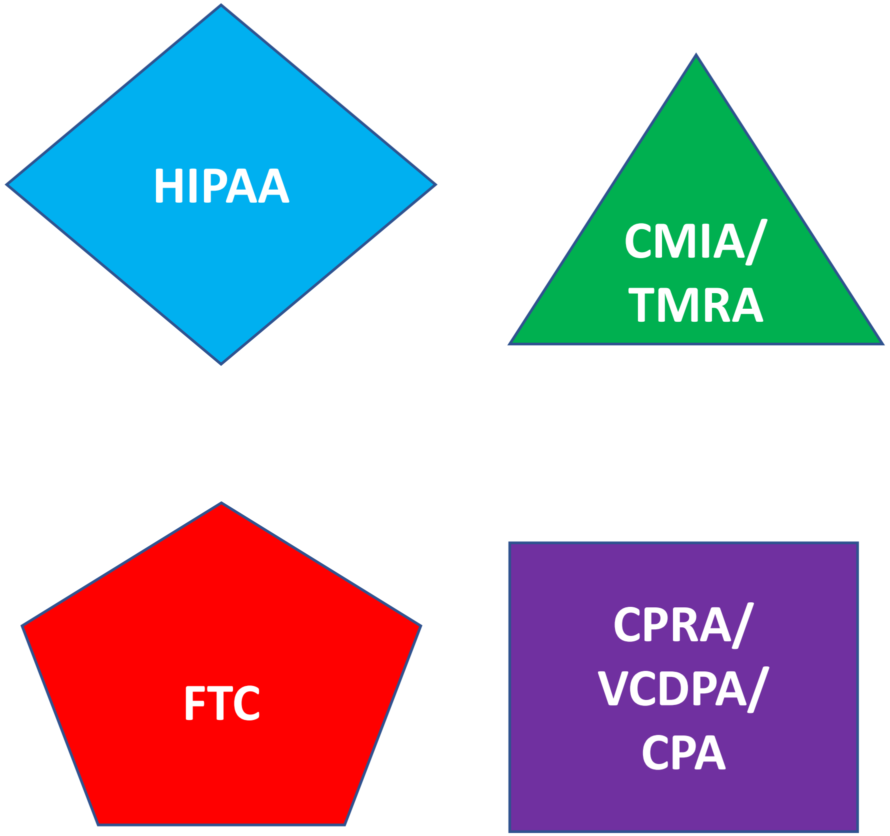
Prior to law school, Mason was an 8th Grade U.S. History teacher and History Department Head at Aiea Intermediate School in Aiea, Hawaii through Teach for America.

mason@hintzelaw.com
W: (281) 849-6281

Agenda

- 12:00
  - HIPAA
    - When it Applies and When it Doesn’t
    - HIPAA Basics
  - State Medical Privacy Laws
  - State Comprehensive Consumer Privacy Laws
  - FTC Health Privacy
  - Other Laws to Consider
  - Q&A
- 1:00

Health information is governed by a variety of laws across jurisdictions.



HIPAA

CMIA/ TMRA

FTC

CPRA/ VCDPA/ CPA

The challenge: What law applies when?

Health Info

HIPAA applies only in very specific situations.

1) Is the entity covered by HIPAA?

Covered Entity (CE):

- Health providers that engage in HIPAA standard electronic transactions
- Health plans
- Healthcare clearinghouses

Business Associate (BA):

- Perform functions on behalf of, or provide services to, Covered Entity (CE) or Business Associate (BA) ***and***
- Create, receive, maintain or transmit (access) PHI for or on behalf of CE or BA

HIPAA applies only in very specific situations.

2) Is there PHI?

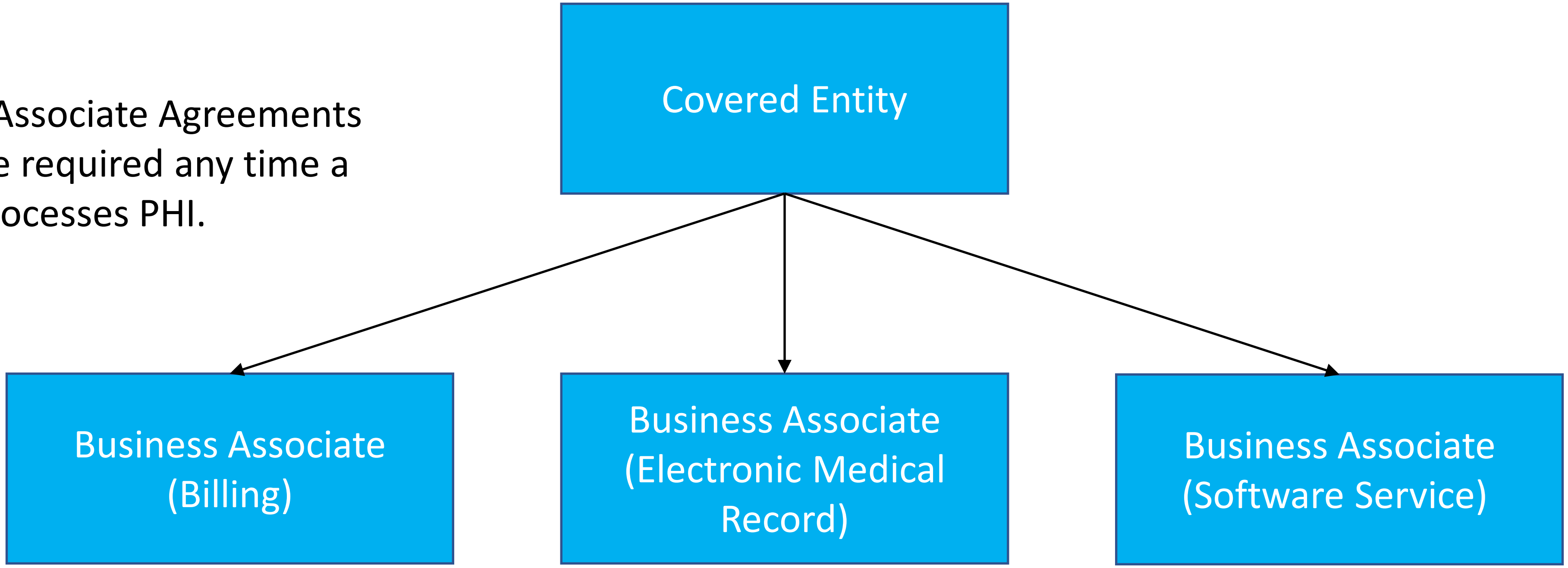
1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse and

2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and

3) Identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual

HIPAA obligations follow the PHI.

Business Associate Agreements (BAAs) are required any time a vendor processes PHI.



Covered Entity

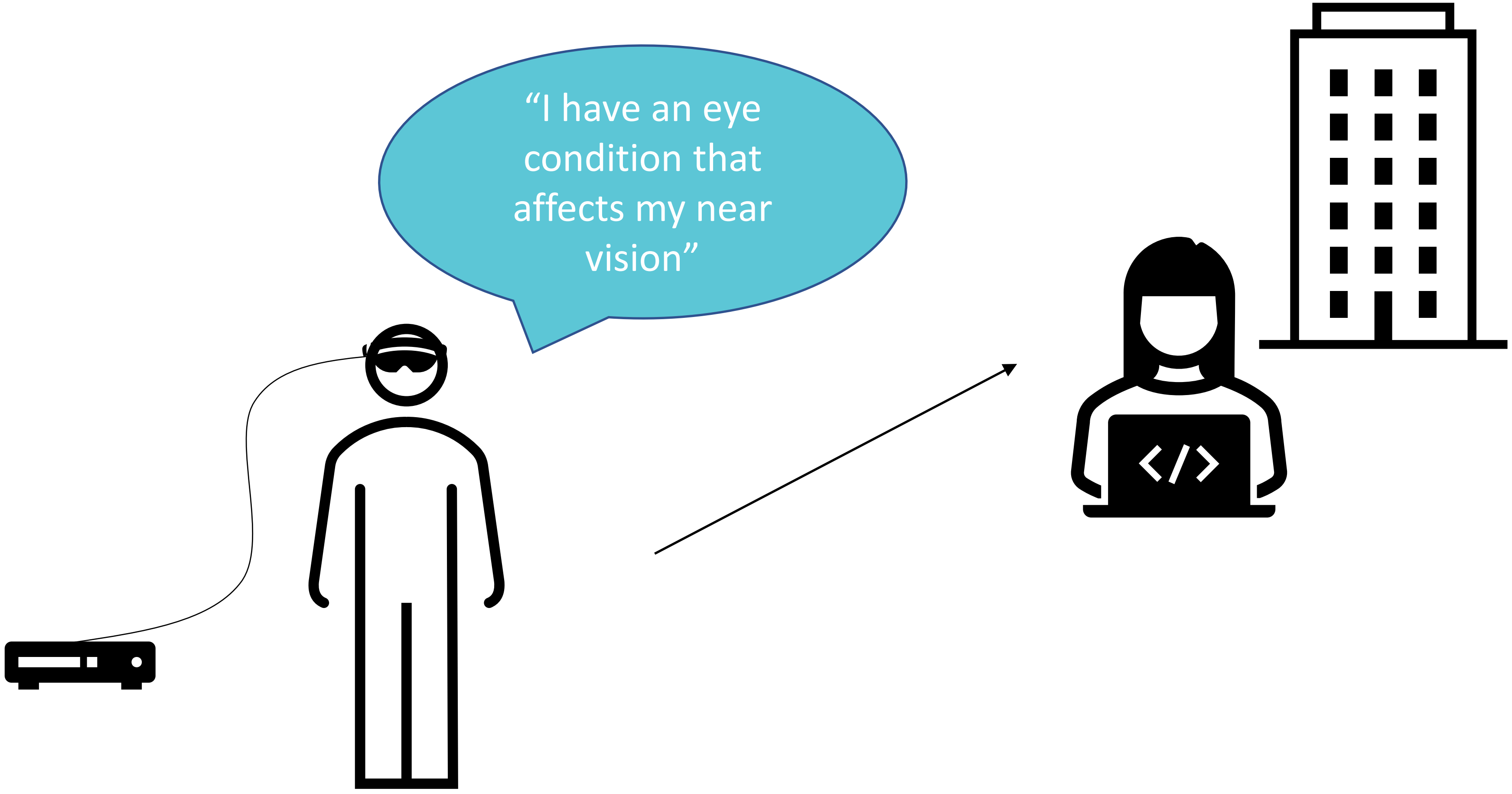
Business Associate (Billing)

Business Associate (Electronic Medical Record)

Business Associate (Software Service)

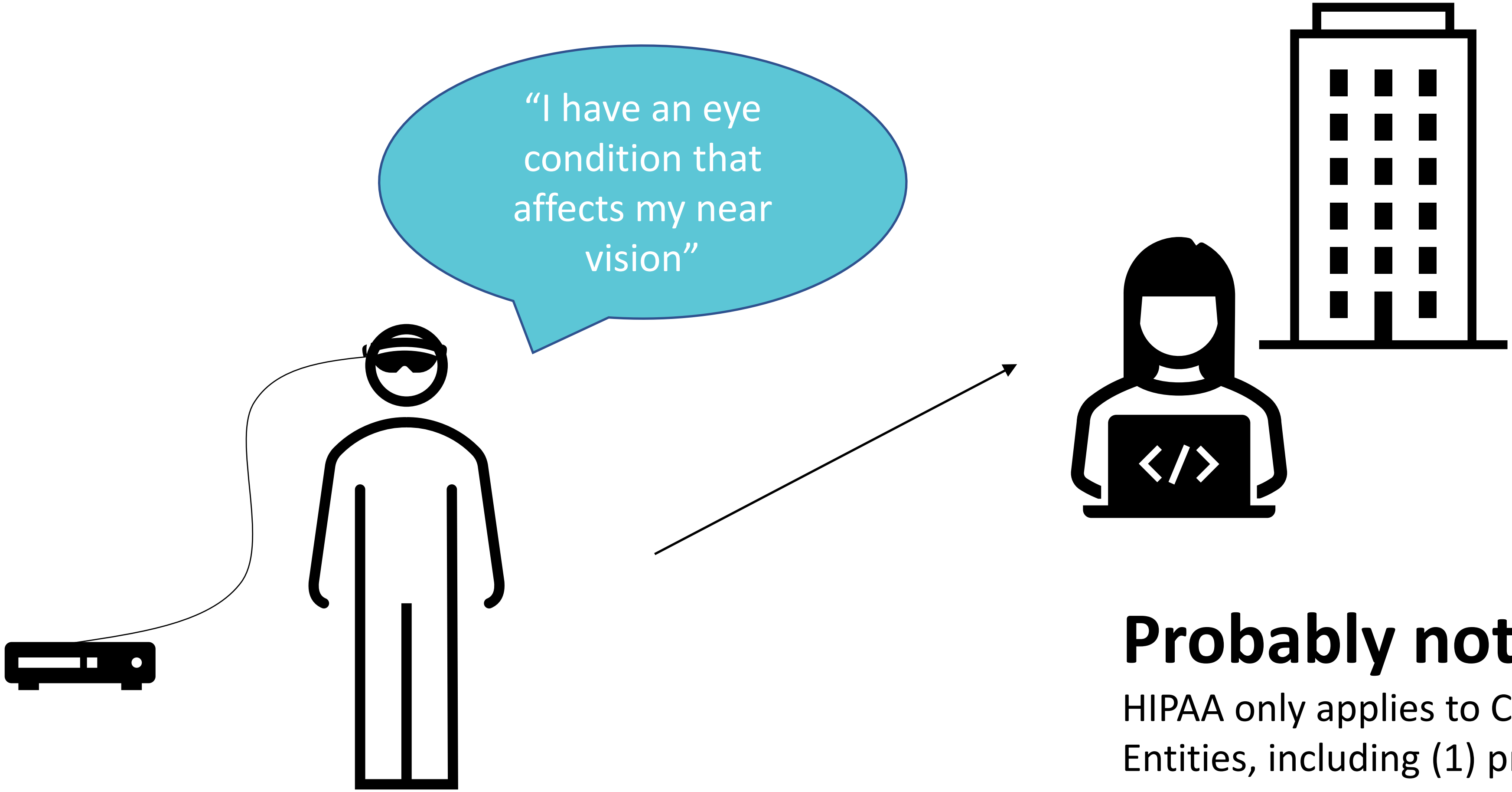
Business Associates are directly covered by HIPAA (i.e., obligations are not only through BAA) for some requirements.

Does HIPAA apply?



"I have an eye condition that affects my near vision"

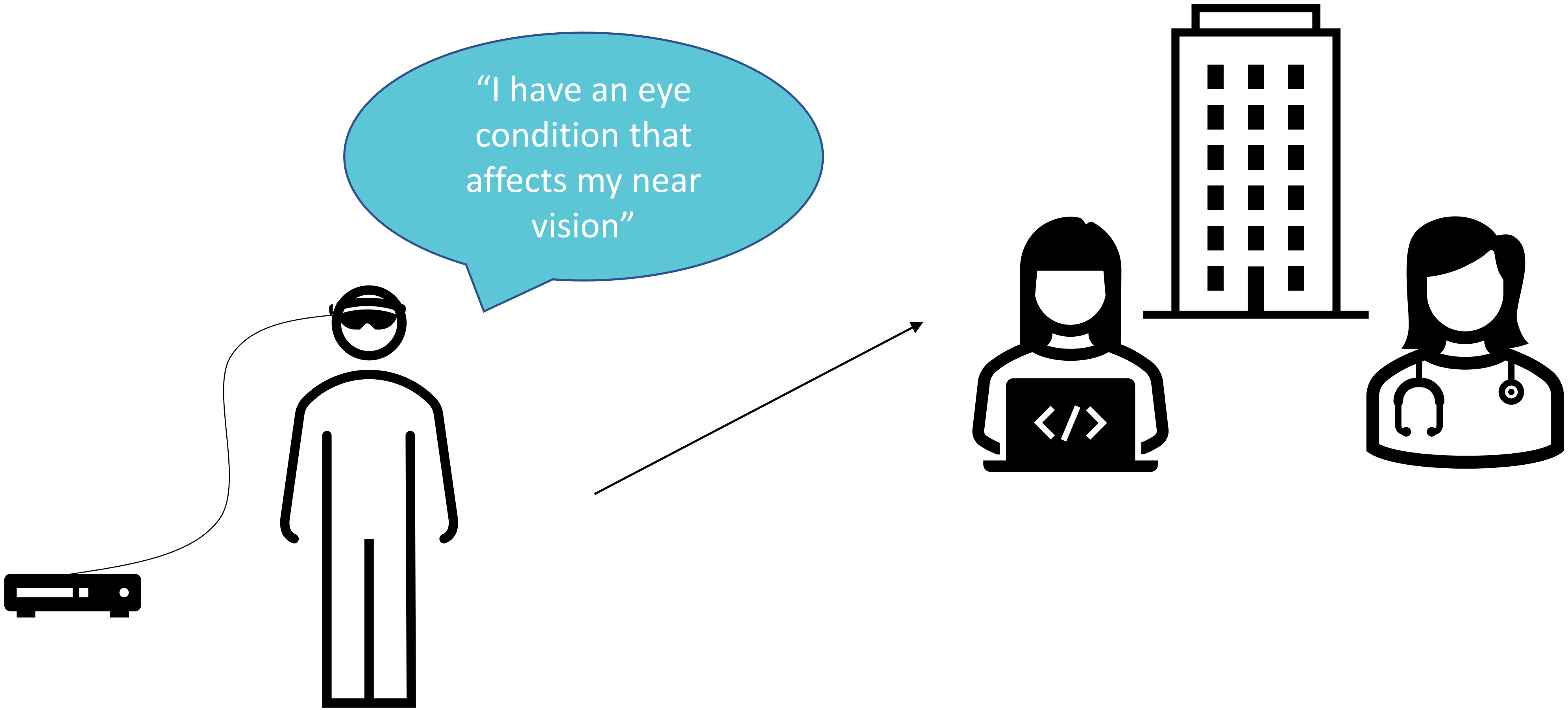
Does HIPAA apply?



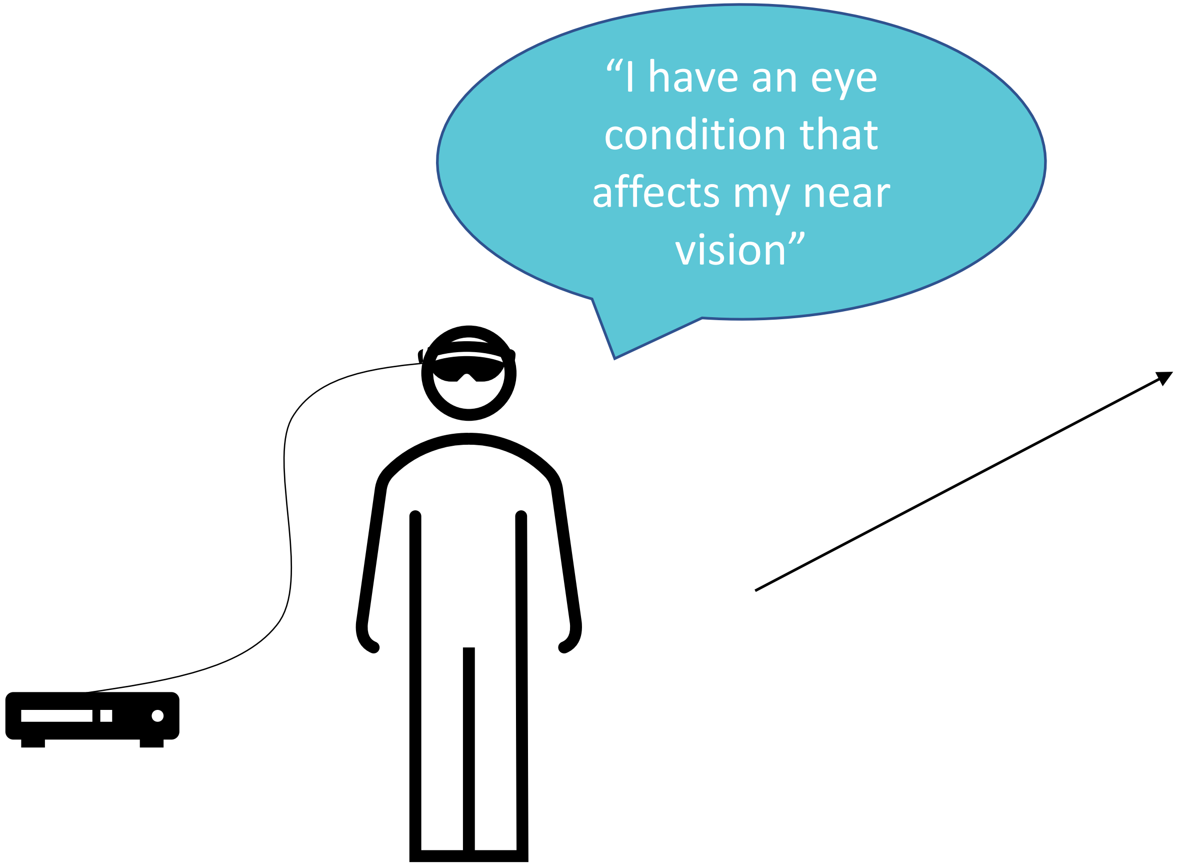
Probably not.

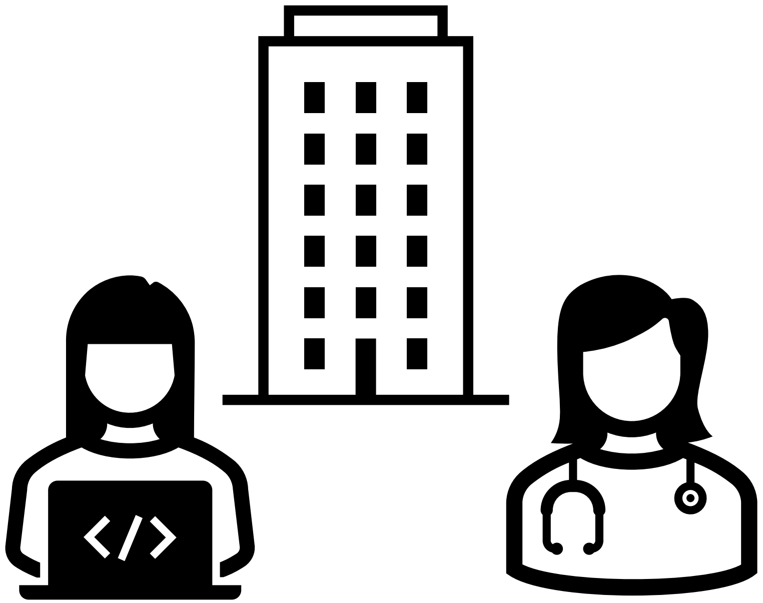
HIPAA only applies to Covered Entities, including (1) providers, (2) health plans, and (3) healthcare clearinghouses.

Does HIPAA apply?



Does HIPAA apply?

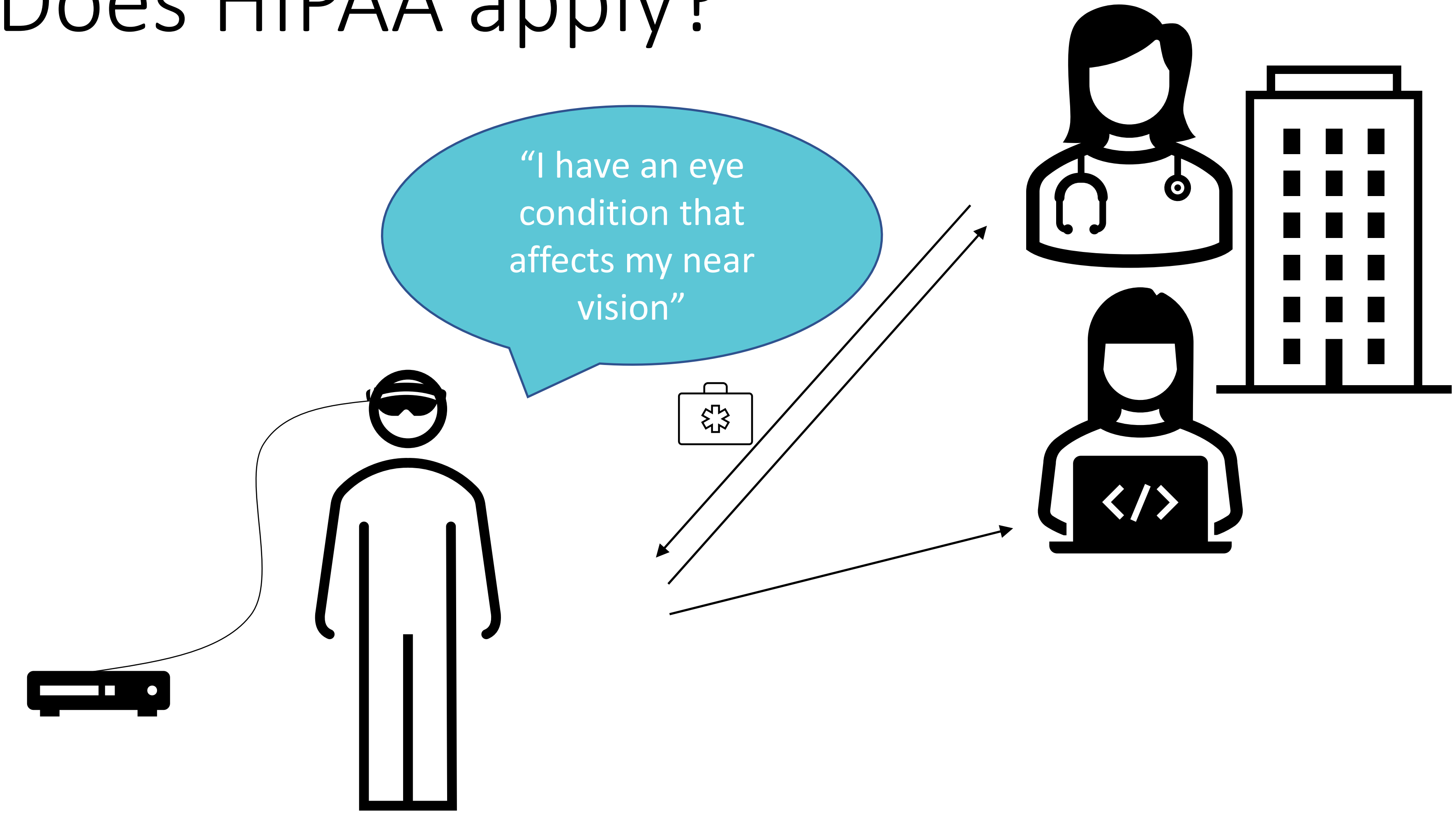




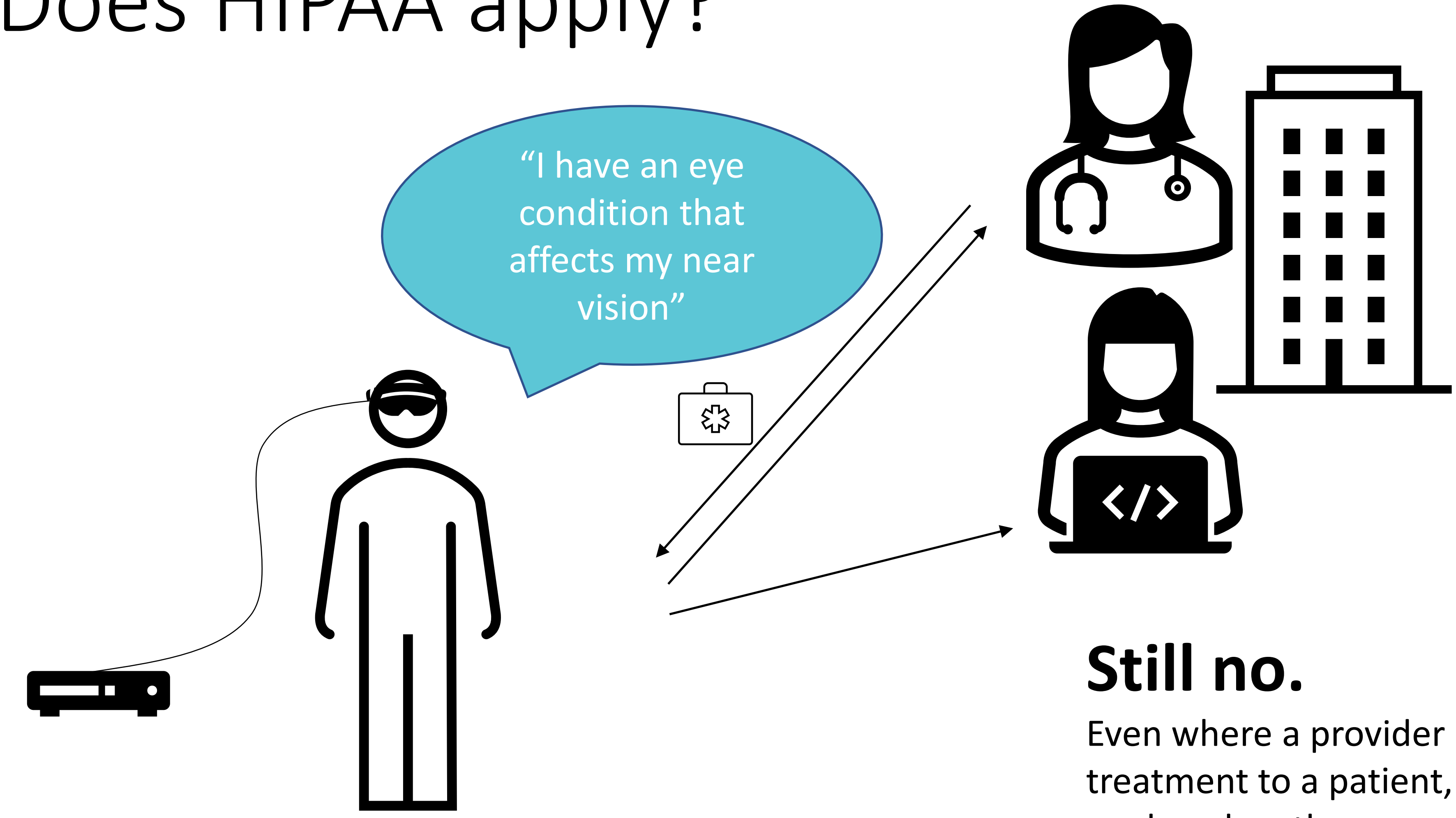
Still probably not.

Even if a healthcare provider is involved, e.g. as a consultant, HIPAA only attaches when they engage in standard transactions.

Does HIPAA apply?



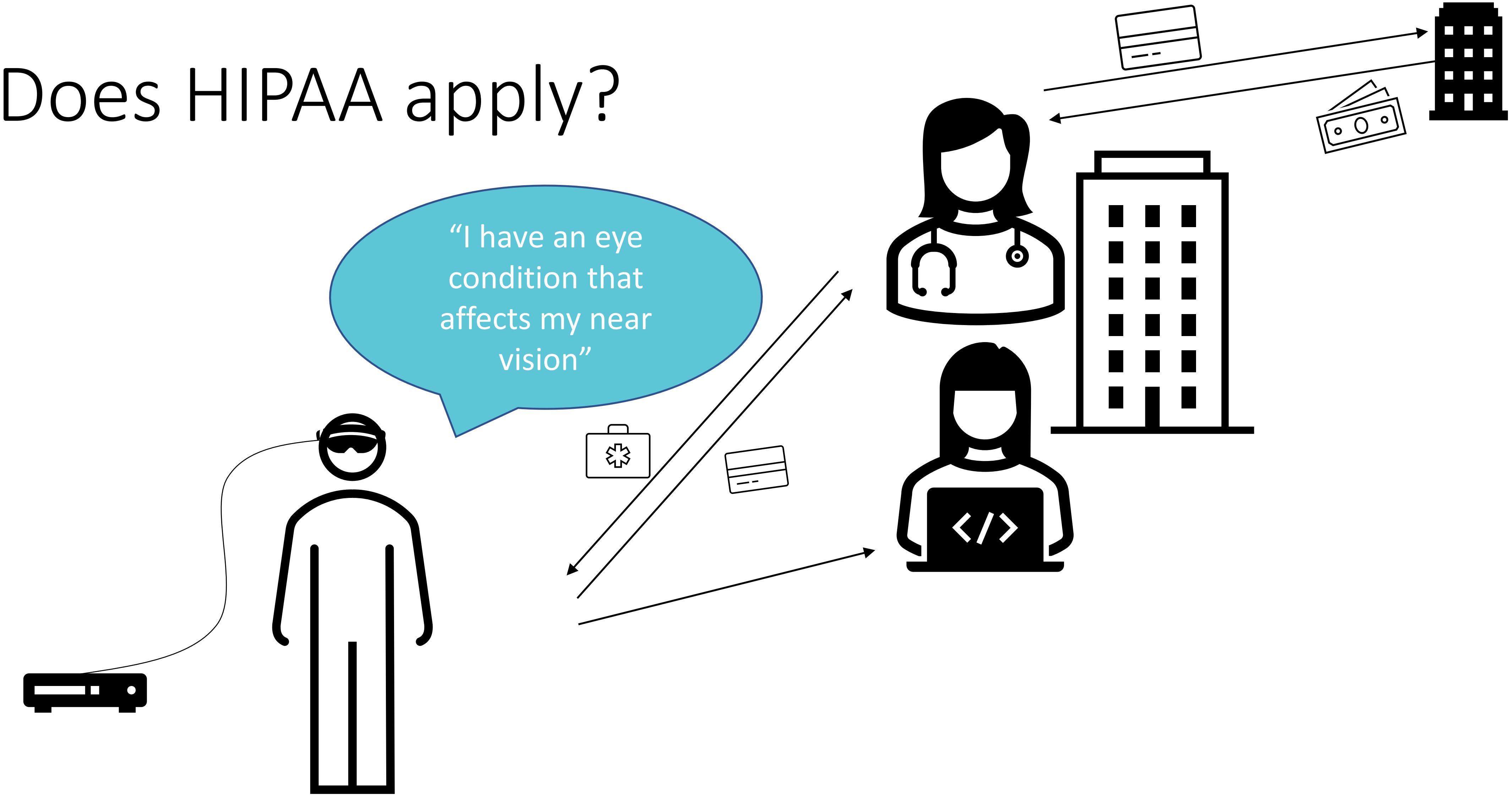
Does HIPAA apply?



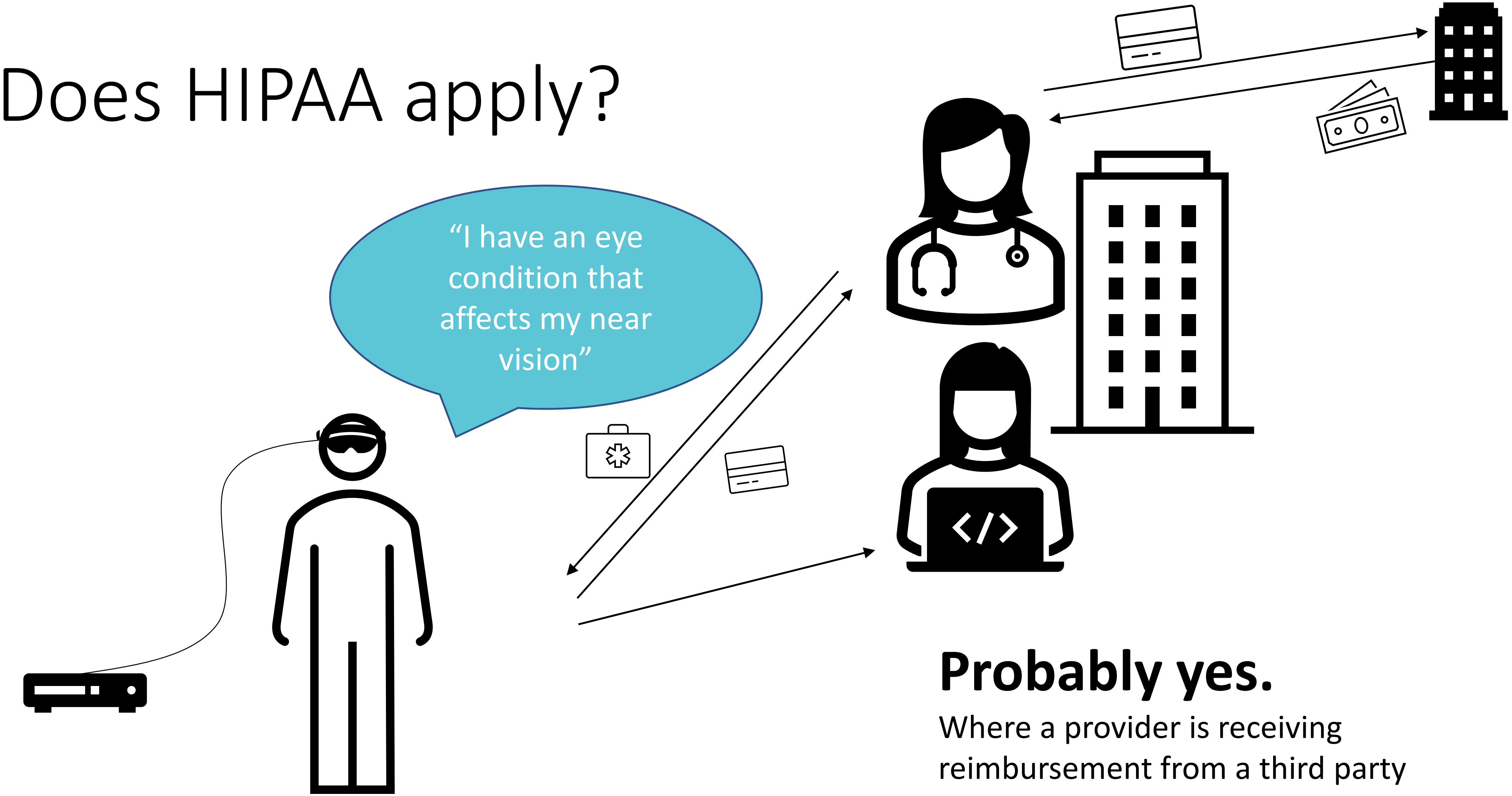
Still no.

Even where a provider is providing treatment to a patient, HIPAA doesn't apply unless there are standard transactions involved.

Does HIPAA apply?



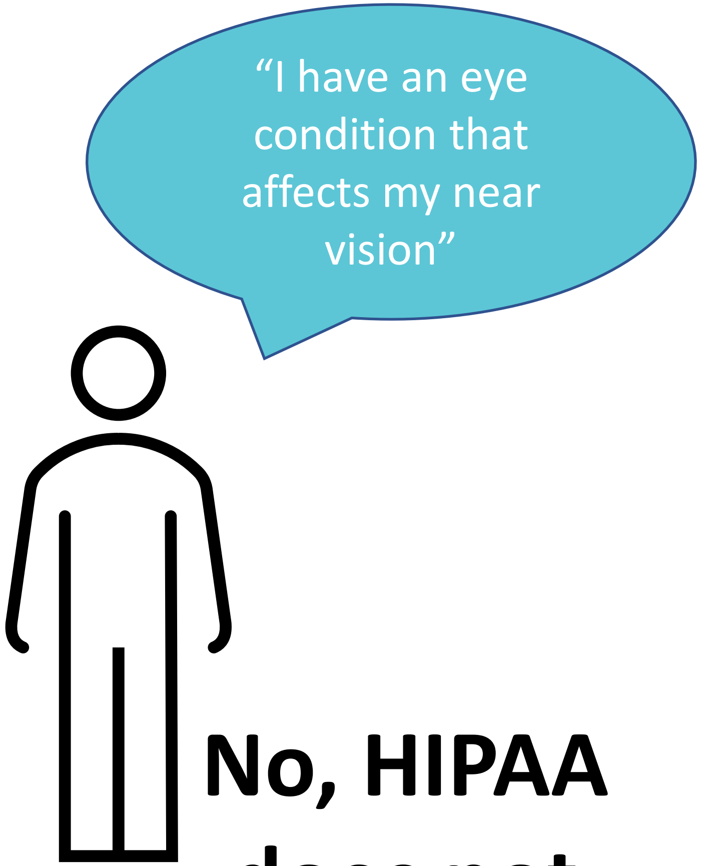
Does HIPAA apply?



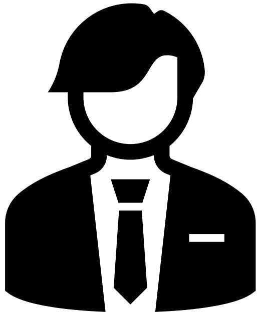
Probably yes.

Where a provider is receiving reimbursement from a third party payer, they become a Covered Entity.

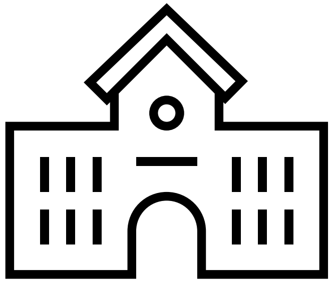
Does HIPAA apply?



No, HIPAA does not apply!

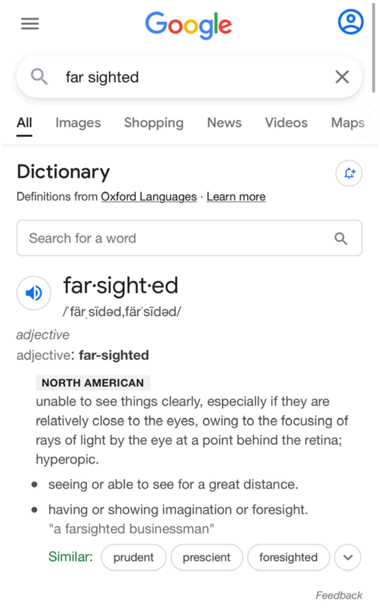


Employer



School

Police/Security



Dictionary

Definitions from Oxford Languages · Learn more

far·sight·ed

/ˈfärˌsīdəd,färˈsīdəd/

adjective

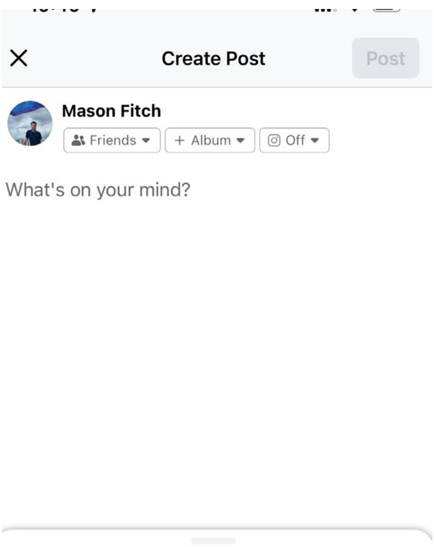
adjective: **far-sighted**

NORTH AMERICAN

unable to see things clearly, especially if they are relatively close to the eyes, owing to the focusing of rays of light by the eye at a point behind the retina; hyperopic.

- seeing or able to see for a great distance.
- having or showing imagination or foresight.
  "a farsighted businessman"

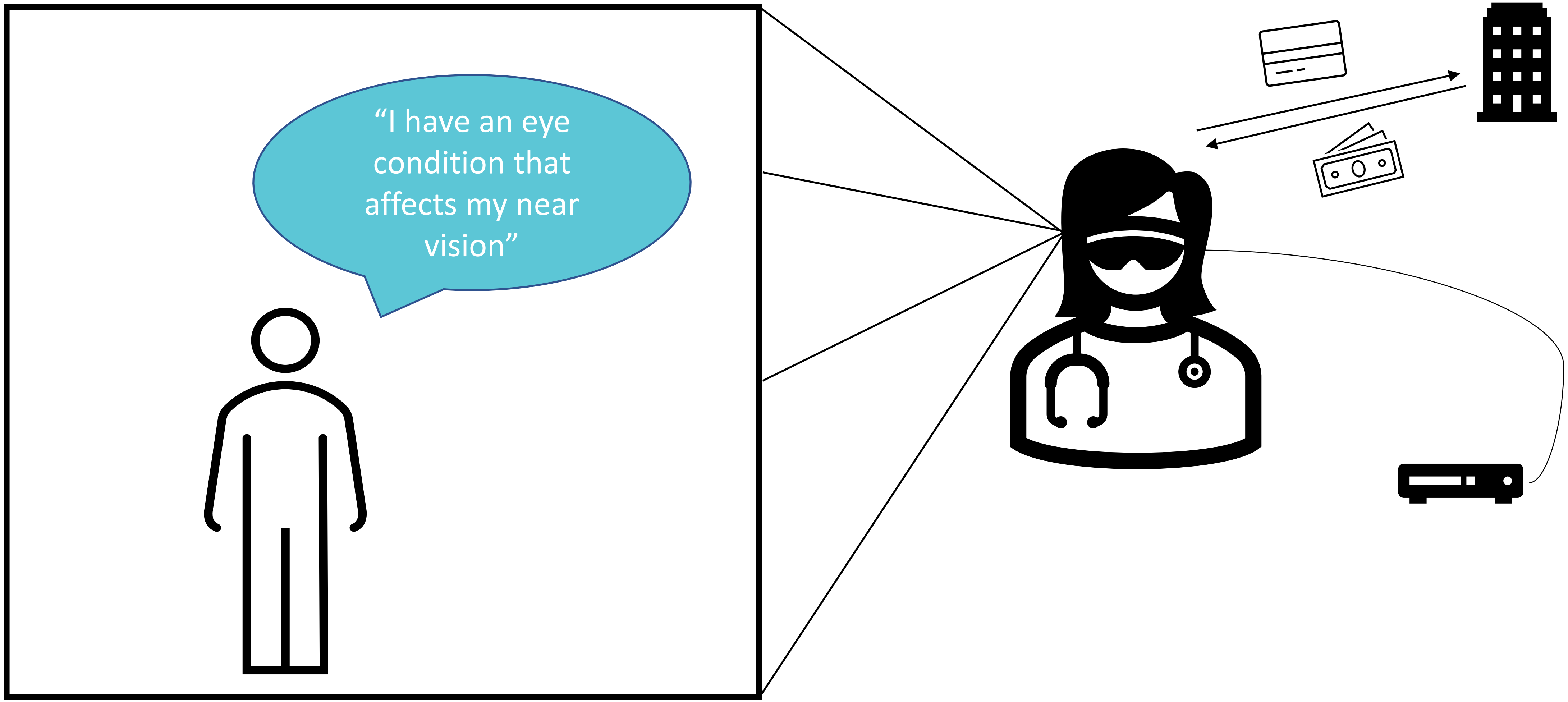
Similar: prudent prescient foresighted



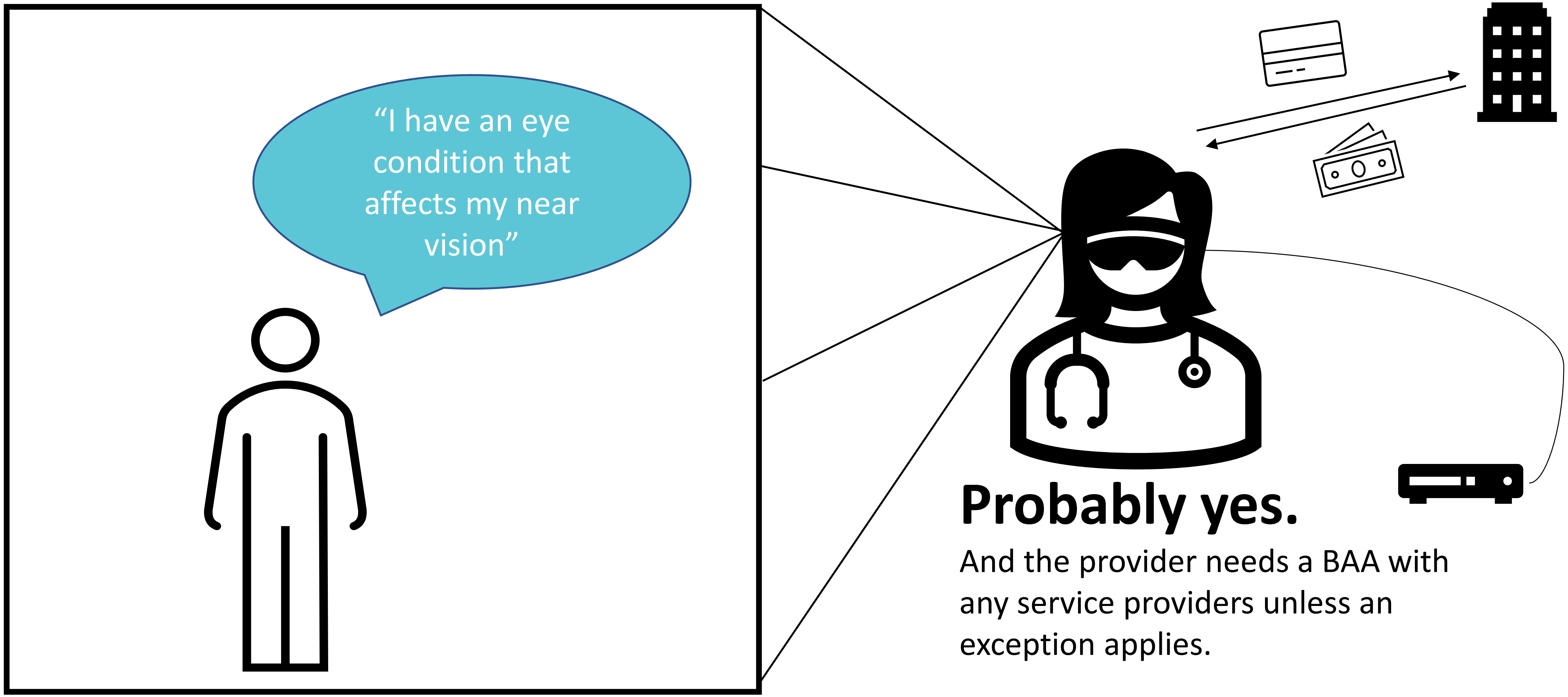
Mason Fitch

What's on your mind?

Does HIPAA apply?



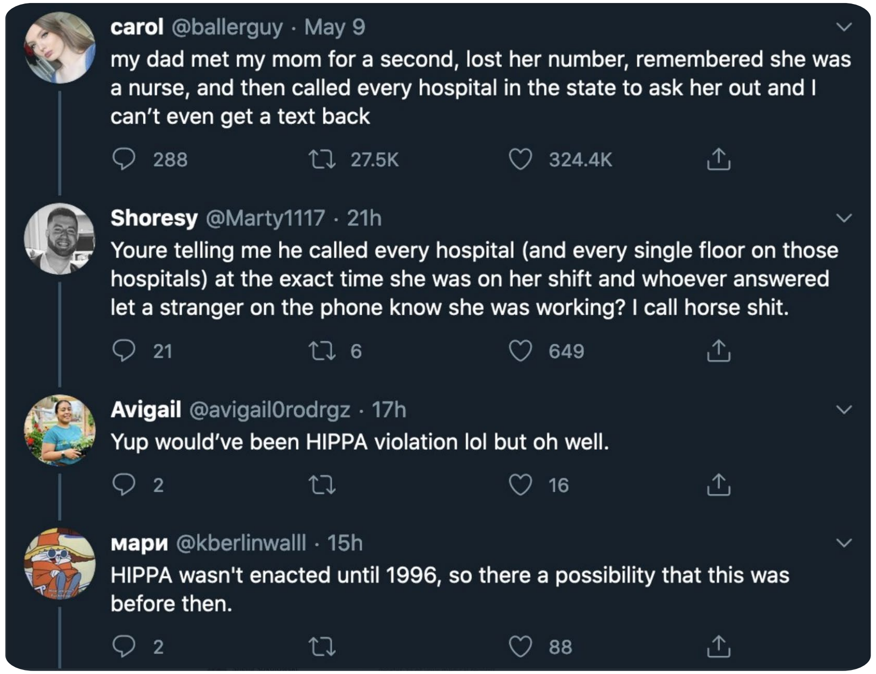
Does HIPAA apply?



Probably yes.

And the provider needs a BAA with any service providers unless an exception applies.

Spot the inaccuracy…



carol @ballerguy · May 9

my dad met my mom for a second, lost her number, remembered she was a nurse, and then called every hospital in the state to ask her out and I can't even get a text back

288 27.5K 324.4K

Shoresy @Marty1117 · 21h

Youre telling me he called every hospital (and every single floor on those hospitals) at the exact time she was on her shift and whoever answered let a stranger on the phone know she was working? I call horse shit.

21 6 649

Avigail @avigail0rodrgz · 17h

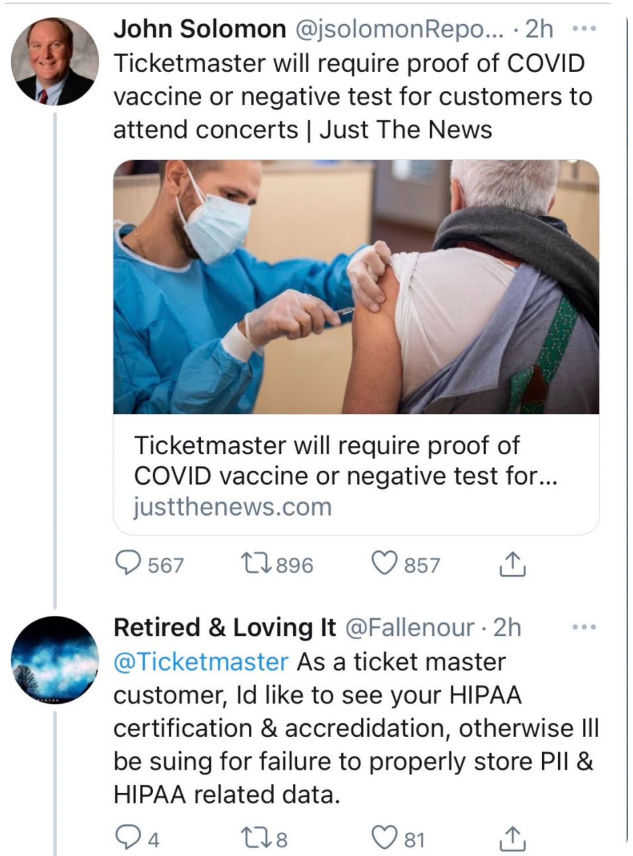
Yup would've been HIPPA violation lol but oh well.

2 16

мари @kberlinwalll · 15h

HIPPA wasn't enacted until 1996, so there a possibility that this was before then.

2 88



John Solomon @jsolomonRepo... · 2h

Ticketmaster will require proof of COVID vaccine or negative test for customers to attend concerts | Just The News

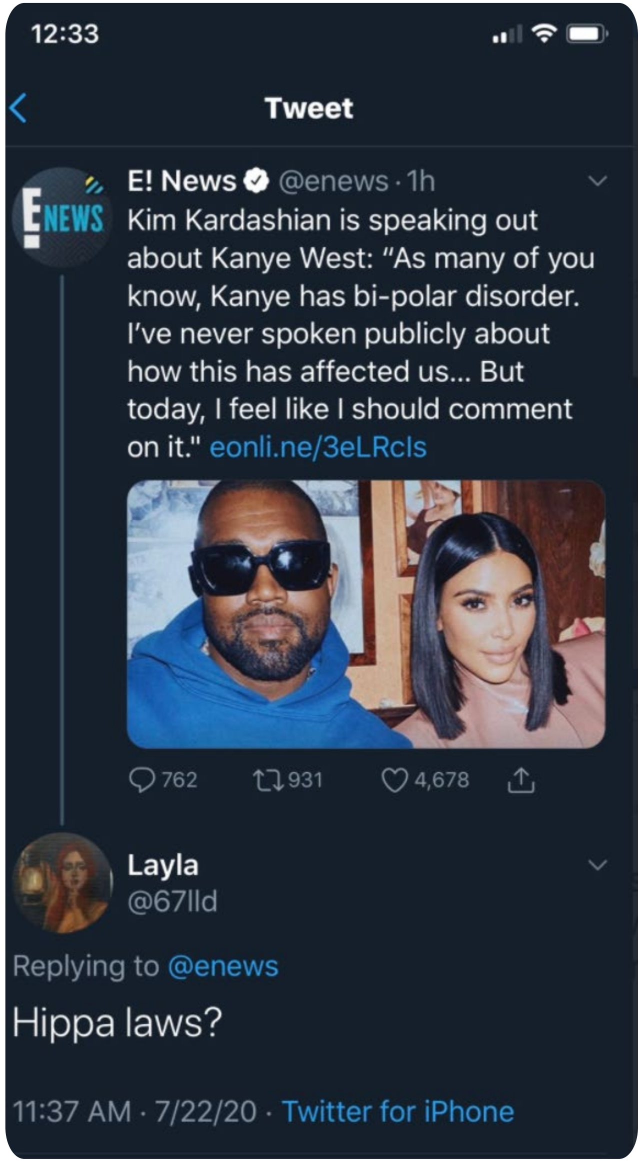
Ticketmaster will require proof of COVID vaccine or negative test for...
justthenews.com

567 896 857

Retired & Loving It @Fallenour · 2h

@Ticketmaster As a ticket master customer, Id like to see your HIPAA certification & accredidation, otherwise Ill be suing for failure to properly store PII & HIPAA related data.

4 8 81



12:33

Tweet

E! News @enews · 1h

Kim Kardashian is speaking out about Kanye West: "As many of you know, Kanye has bi-polar disorder. I've never spoken publicly about how this has affected us... But today, I feel like I should comment on it." eonli.ne/3eLRcls

762 931 4,678

Layla
@67lld

Replying to @enews

Hippa laws?

11:37 AM · 7/22/20 · Twitter for iPhone

Hintze Law
Privacy + Data Security

Once it applies, HIPAA is prescriptive.

Privacy Rule

Defines permitted uses for which authorization is not required:

- Treatment
- Payment
- Healthcare operation

Defines uses for which authorization is required:

- Marketing
- Sale
- Anything other than permitted TPO uses

+ Much more

Security Rule

Prescribes mandatory and addressable security components, both programmatic and technical. E.g., annual risk assessment and encryption of PHI.

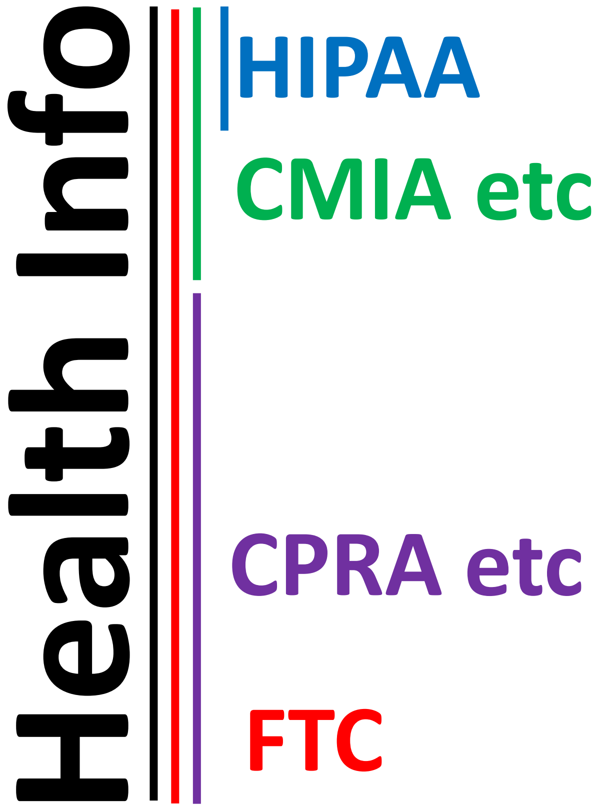
+ Much more

If HIPAA has such limited coverage, what fills the gaps?

Health Info

HIPAA

In the US, several laws apply to the broader category of health info.



Health Info

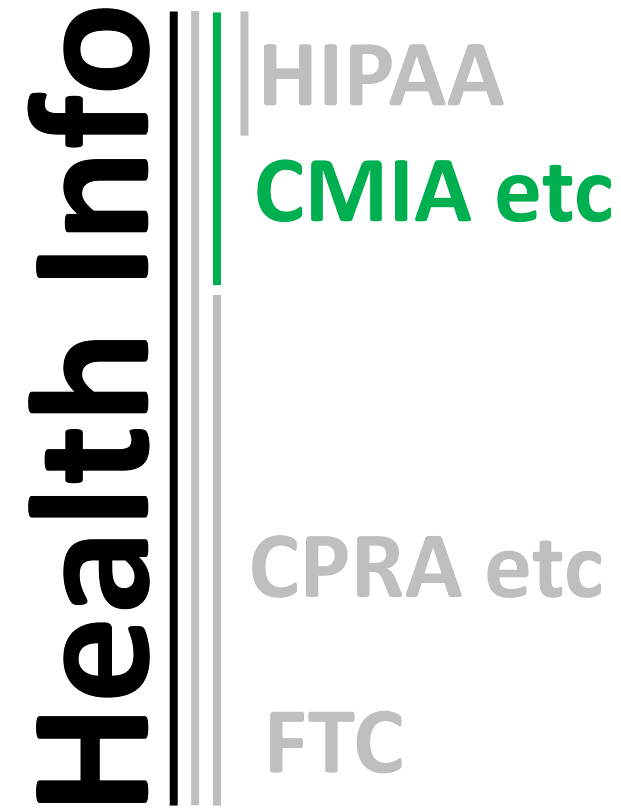
HIPAA

CMIA etc

CPRA etc

FTC

In the US, several laws apply to the broader category of health info.



Health Info

HIPAA

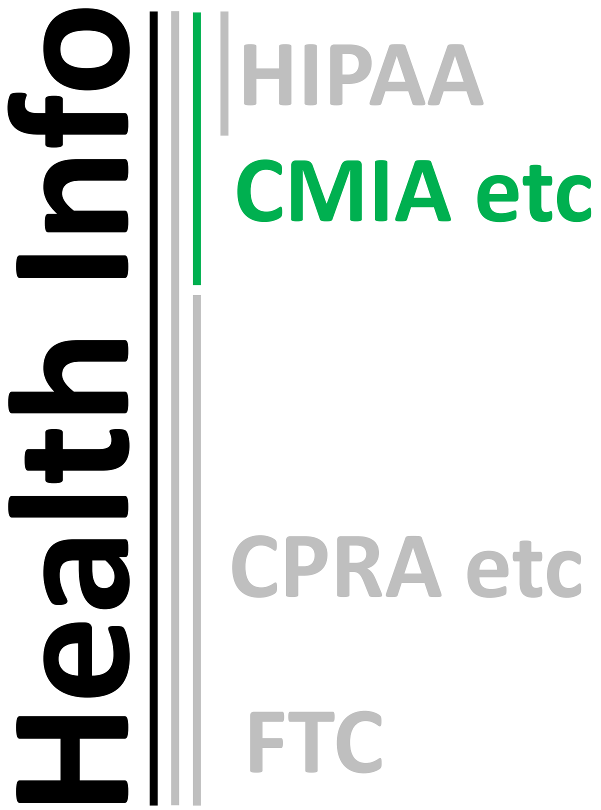
CMIA etc

CPRA etc

FTC

- Many states have health privacy laws that overlap with HIPAA, e.g., the **Texas Medical Records Privacy Act and the California Confidentiality of Medical Information Act**
- Apply to “medical information” handled by providers and plans regardless of type of transaction
  - CMIA: “’Medical information’ means any individually identifiable information, in electronic or physical form, **in possession of or derived from a provider of health care**, health care service plan, pharmaceutical company, or contractor **regarding a patient’s medical history, mental or physical condition, or treatment.**”
  - TMAP: Applies to “PHI” held by “covered entities,” but CE has a vastly broader definition under state law (“person who maintains an internet site”)
- Apps that store medical information are “providers” subject to CMIA

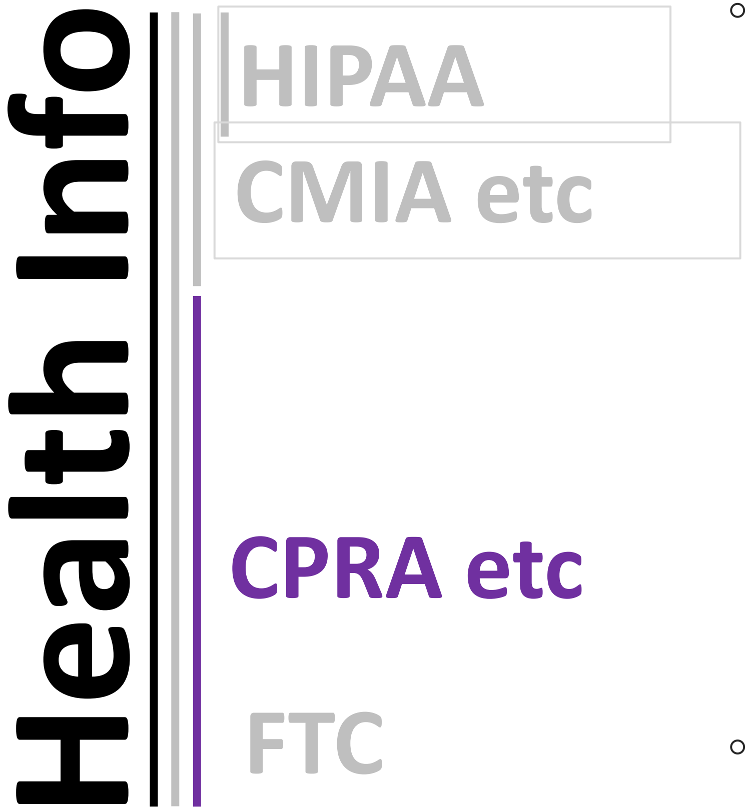
In the US, several laws apply to the broader category of health info.



- HIPAA preempts state laws <u>except</u> where state law provides stronger protection
  - CMIA includes a private right of action for breaches
  - NY requires fulfillment of access request within 10 days, as compared to 30 days under HIPAA
  - TX has more restrictive marketing rules
- Glow enforcement: CA AG obtained $250,000 settlement under CMIA based on security flaws and inappropriate disclosure of non-PHI health info.

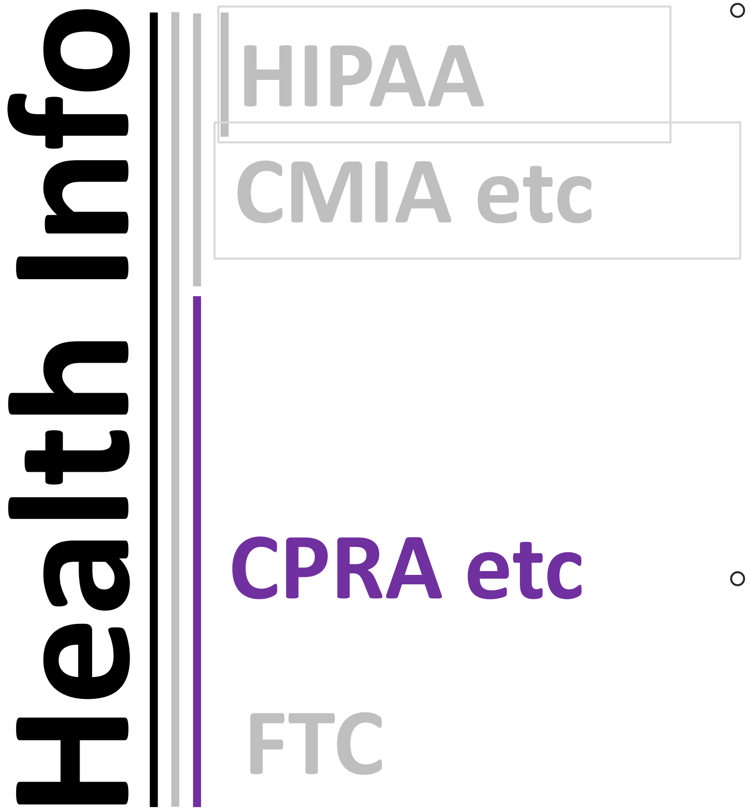
Hintze Law
Privacy + Data Security

In the US, several laws apply to the broader category of health info.



- Comprehensive consumer privacy laws include protections for a far broader swath of health data
  - CPRA: “sensitive personal information” includes “personal information collected and analyzed concerning a consumer’s health”
  - VCDPA: “sensitive data” includes “personal data revealing mental or physical health diagnosis”
  - CPA: “sensitive data” includes “personal data revealing … a mental or physical health condition or diagnosis”
  - CT: “sensitive data” includes “data revealing … mental or physical health condition or diagnosis”
- Exclude data covered by HIPAA/CMIA

In the US, several laws apply to the broader category of health info.



Health Info

HIPAA

CMIA etc

CPRA etc

FTC

- What data is exempted?
  - Most state privacy laws exclude data governed by other health laws
  - CPRA Exemptions
    - Medical Information (CMIA) or PHI (HIPAA) collected by CE/BA
    - CE under CMIA/HIPAA, to the extent they treat all data as PHI
    - Personal information collected under Common Rule
  - Some state laws (e.g., VCDPA) include wholesale exemptions for CE/BAs; drafting error?
- Exemptions can result in CE/BAs being subject to several frameworks based on data type

	CPRA	VCDPA	CPA	CT
Definition	“personal information collected and analyzed concerning a consumer’s health”	“personal data revealing mental or physical health diagnosis”	“personal data revealing … a mental or physical health condition or diagnosis”	“data revealing … mental or physical health condition or diagnosis”
Limitation	Consumer right to direct a business, at any time, to “limit the use and disclosure of … Sensitive PI”	“A controller shall … Not process sensitive data concerning a consumer without obtaining the consumer's consent …”	“A controller shall not process a consumer’s sensitive data without first obtaining consent …”	“A controller shall … not process sensitive data concerning a consumer without obtaining the consumer's consent …”
Additional Requirements	Must disclose categories, purposes, and sold/shared status of sensitive PI Maintain reasonable security	Conduct data protection assessment	Conduct data protection assessment	Conduct data protection assessment

	CPRA	VCDPA	CPA	CT
Definition	“personal information collected and analyzed concerning a consumer’s health”	“personal data revealing mental or physical health diagnosis”	“personal data revealing … a mental or physical health condition or diagnosis”	“data revealing … mental or physical health condition or diagnosis”
Limitation	Consumer right to direct a business, at any time, to “limit the use and disclosure of … Sensitive PI”	“A controller shall … Not process sensitive data concerning a consumer without obtaining the consumer's consent …”	“A controller shall not process a consumer’s sensitive data without first obtaining consent …”	“A controller shall … not process sensitive data concerning a consumer without obtaining the consumer's consent …”
Additional Requirements	Must disclose categories, purposes, and sold/shared status of sensitive PI Maintain reasonable security	Conduct data protection assessment	Conduct data protection assessment	Conduct data protection assessment

What counts as “health” data?

Health Info

HIPAA

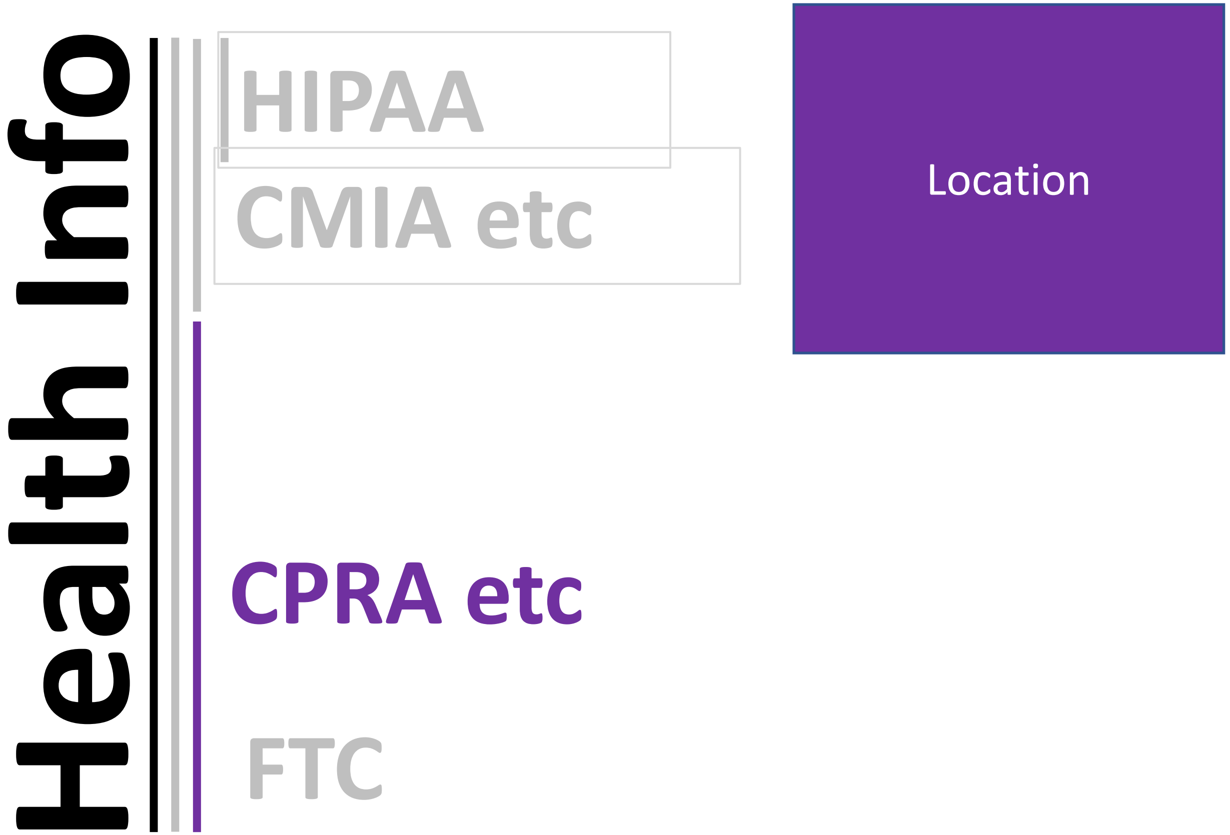
CMIA etc

CPRA etc

FTC

- Location
- Purchases
- Employee temperature checks
- Browsing activity
- Online communities
- Physical Traits

What counts as “health” data?



Health Info

HIPAA

CMIA etc

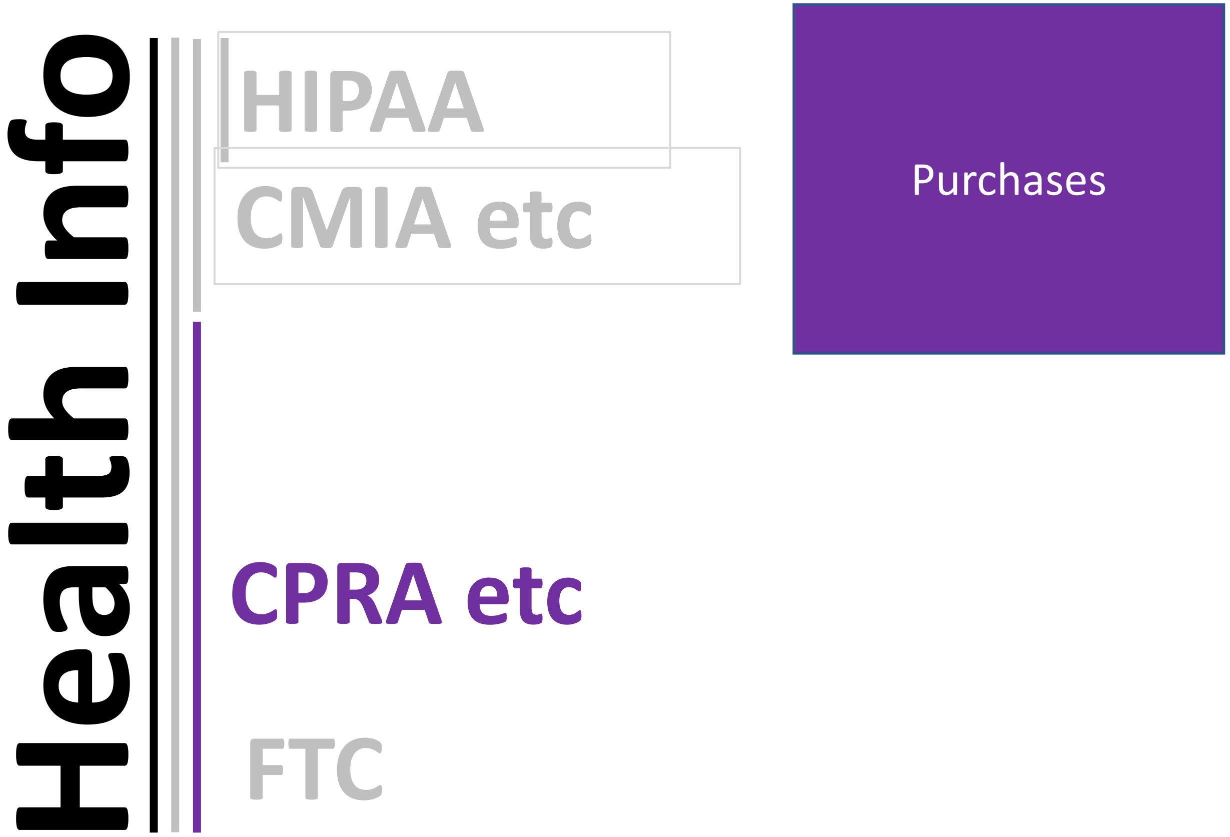
CPRA etc

FTC

Location

- When is location data also health data?
  - If phone constantly tracks location, is hospital location health data?
  - What if you don’t process it to infer health info?
- Example: user location at abortion clinic
  - Geofence for non-health related advertisement (e.g., political ad)?
  - Geofence for health-related advertisement?
  - Profiling?

What counts as “health” data?



Health Info

HIPAA

CMIA etc

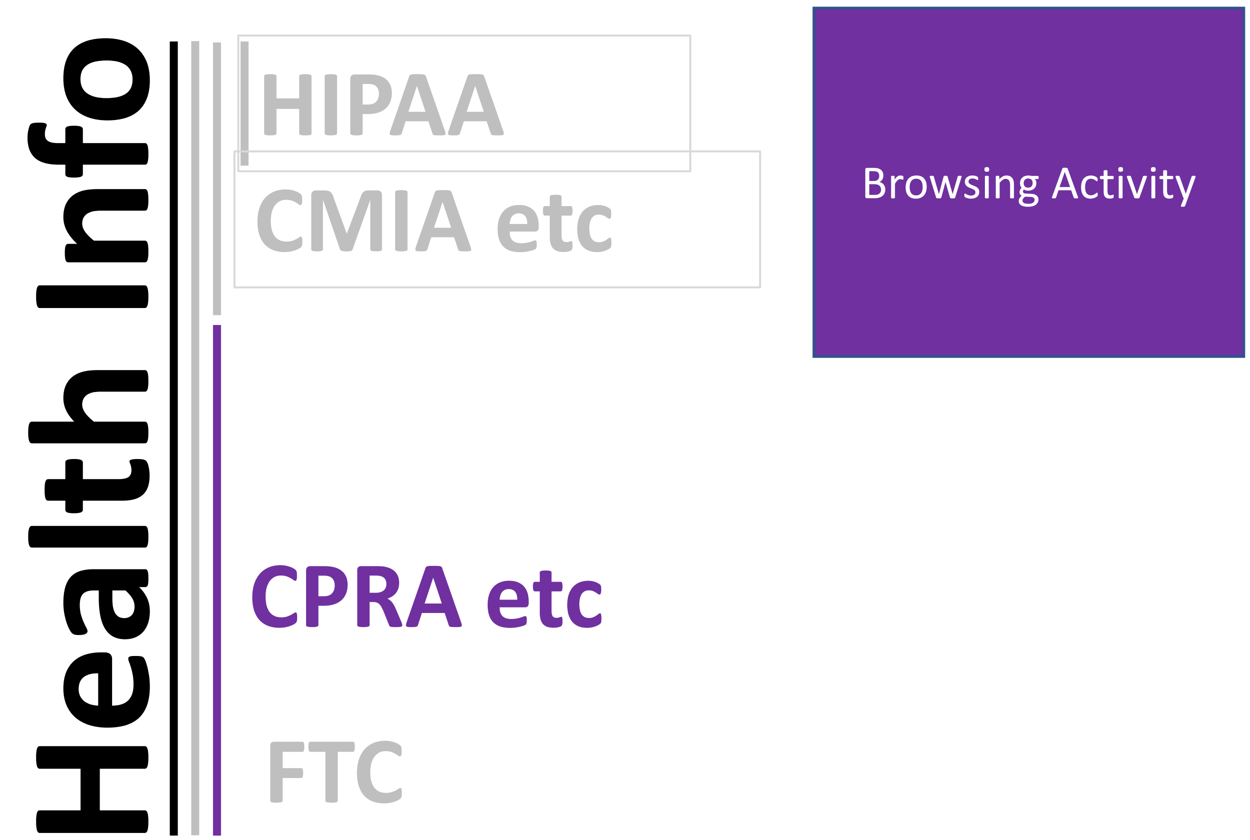
CPRA etc

FTC

Purchases

- Does the purchase of health-related products constitute “health data”?
  - General condition – e.g., Tylenol for headache
  - Widespread condition – e.g., OTC allergy medicines
  - Sensitive and specific – e.g., OTC HIV test
- Possible uses:
  - Grocery store record keeping
  - Rewards programs
  - Targeting

What counts as “health” data?



Health Info

HIPAA

CMIA etc

CPRA etc

FTC

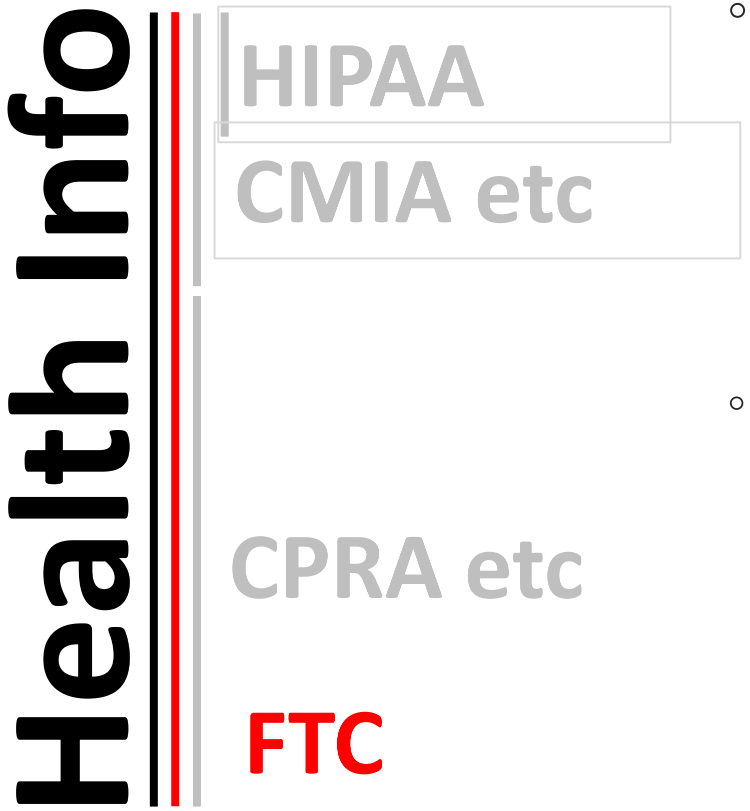
Browsing Activity

- What inferences can be made from browsing a health-oriented site?
  - Is there a difference between “mayoclinic.com/diabetes-101-newly-diagnosed” and searching “diabetes info”?
    - Do either reveal a “condition” or “diagnosis”?
    - Where do you draw the line between “that person has diabetes” and “that person may have diabetes”?
- Does the activity change the type of data?
  - If logging browsing activity is not health data, what if that same data is used to target people?

What counts as “health” data?

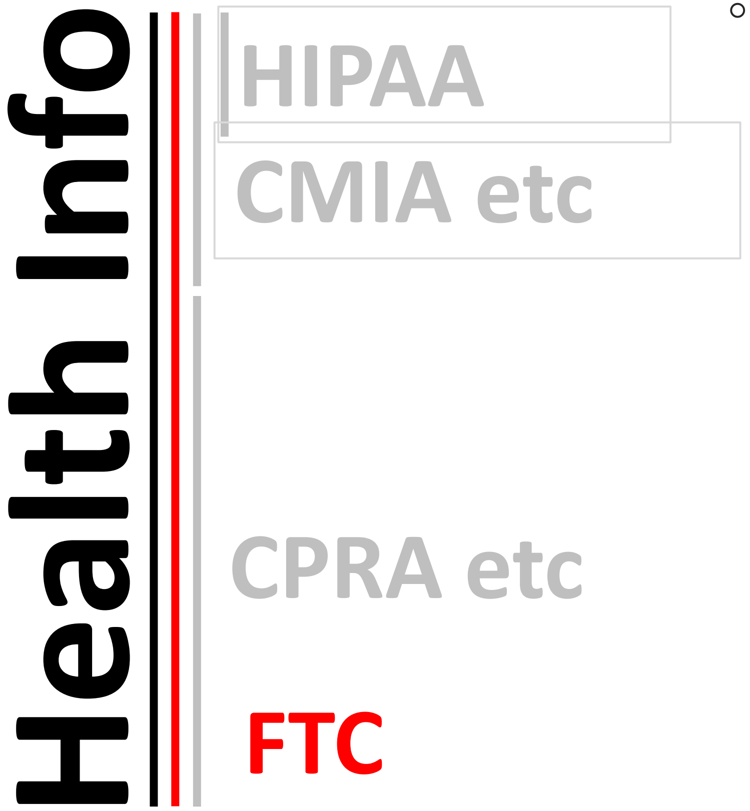
State	Definition	Site Logs	Purchases	Ad targeting
CA	“personal information collected and analyzed concerning a consumer’s health”	N	N	Y
CO	“personal data revealing … a mental or physical health condition or diagnosis”	Y, on some sites	Y?	Y
CT	“data revealing … mental or physical health condition or diagnosis”	Y, on some sites	Y?	Y
VA	“personal data revealing mental or physical health diagnosis”	Y, on some sites	Y?	Y?

The FTC has jurisdiction across the health data spectrum.



- FTC has deceptive/unfair coverage of healthcare entities, regardless of whether or not HIPAA applies
  - Flo settlement alleged deceptive statements relating to handling and sharing of health information, namely fertility tracking
  - Has published guidance on mobile health app privacy + signaled interest in health privacy
- COPPA: recent enforcement action against WW International emphasized health component
  - Tracked weight, food intake, activity, etc.

The FTC has jurisdiction across the health data spectrum.



Health Info

HIPAA

CMIA etc

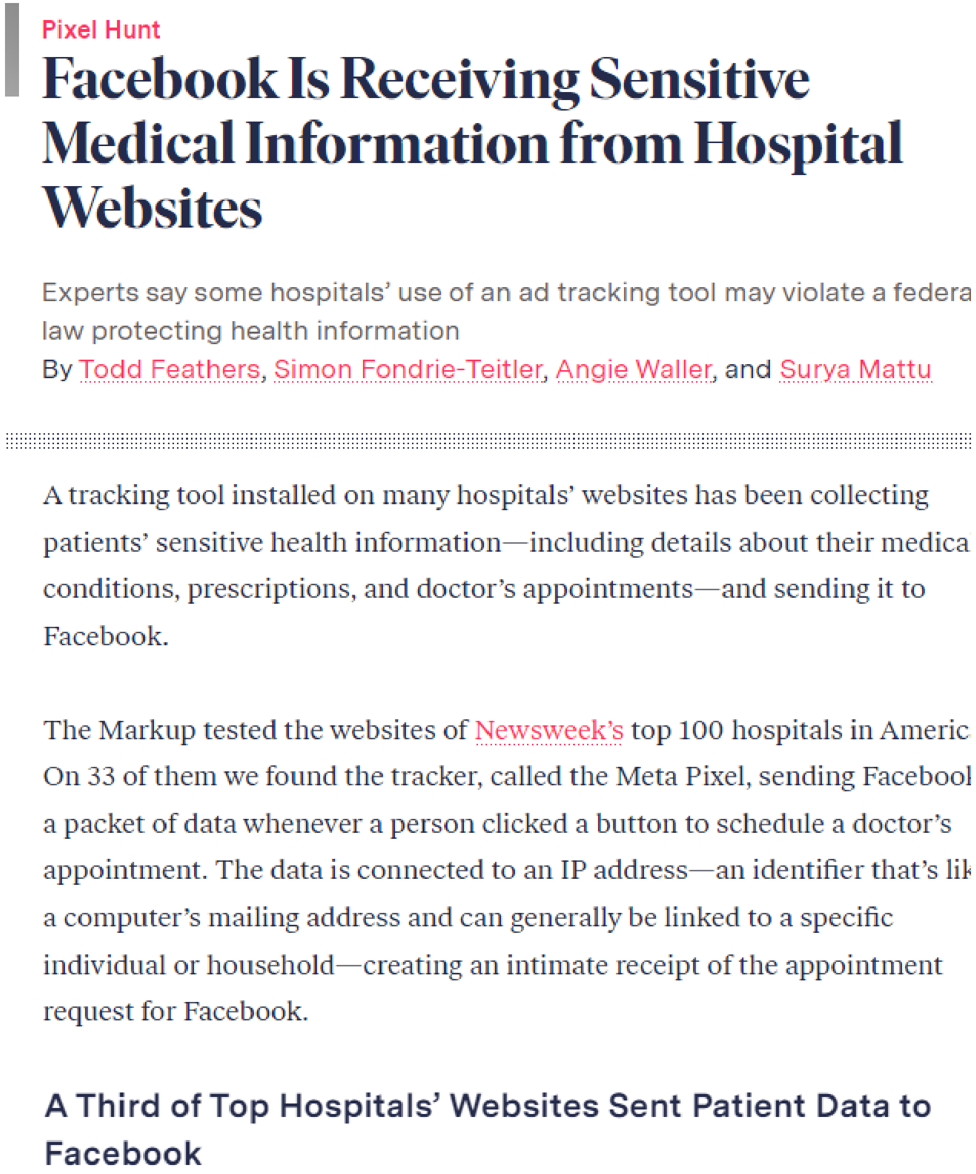
CPRA etc

FTC

- Health Breach Notification Rule
  - Passed in 2009, but 2021 FTC Policy Statement noted increased need for enforcement
  - Applies to vendors of “personal health records,” very broadly defined
  - “Breach” is also broadly defined – includes sharing without user authorization
  - Only applies to entities not subject to HIPAA
  - Requires notice to individual and FTC, and possibly the media

Example: Mass Gen Cookies Settlement

- Mass Gen was sued under MA breach of privacy law (amid other claims, which were dismissed) for disclosing patient data via pixels (e.g., Facebook Pixel and Google Tag Manager)
  - Tags recorded events such as "/search/q=colon+cancer+treatment+" alongside IP addresses and other identifying info
  - Facebook logged user logging into Patient Gateway
  - Other events logged include "appointments" and "display=new patients"
- Mass Gen used an iFrame, but also appeared to have Advanced Matching turned on (which scrapes PII from field sites)
- Emphasizes potential breadth of health data on sites, plus risk of exposure to third parties
- Tracks other health-data related issues, such as Glow and Flo settlements, involving disclosure of health data through analytics:
  - Custom event R_PREGNANCY_WEEK_CHOSEN
  - Custom event R_ACCEPT_PUSHES_PERIOD



Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Experts say some hospitals' use of an ad tracking tool may violate a federa law protecting health information

By Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu

A tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information—including details about their medica conditions, prescriptions, and doctor's appointments—and sending it to Facebook.

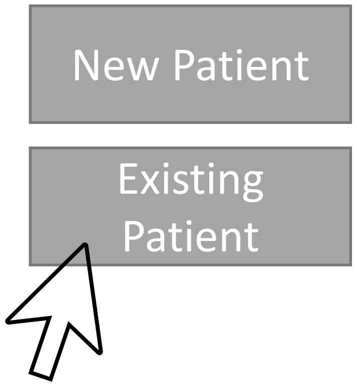
The Markup tested the websites of Newsweek's top 100 hospitals in Americ On 33 of them we found the tracker, called the Meta Pixel, sending Faceboo a packet of data whenever a person clicked a button to schedule a doctor's appointment. The data is connected to an IP address—an identifier that's lik a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook.

A Third of Top Hospitals' Websites Sent Patient Data to Facebook

On the website of University Hospitals Cleveland Medical Center, for example, clicking the "Schedule Online" button on a doctor's page prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the search term we used to find her: "pregnancy termination."

Clicking the "Schedule Online Now" button for a doctor on the website of Froedtert Hospital, in Wisconsin, prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the condition we selected from a dropdown menu: "Alzheimer's."

What data gets sent where?

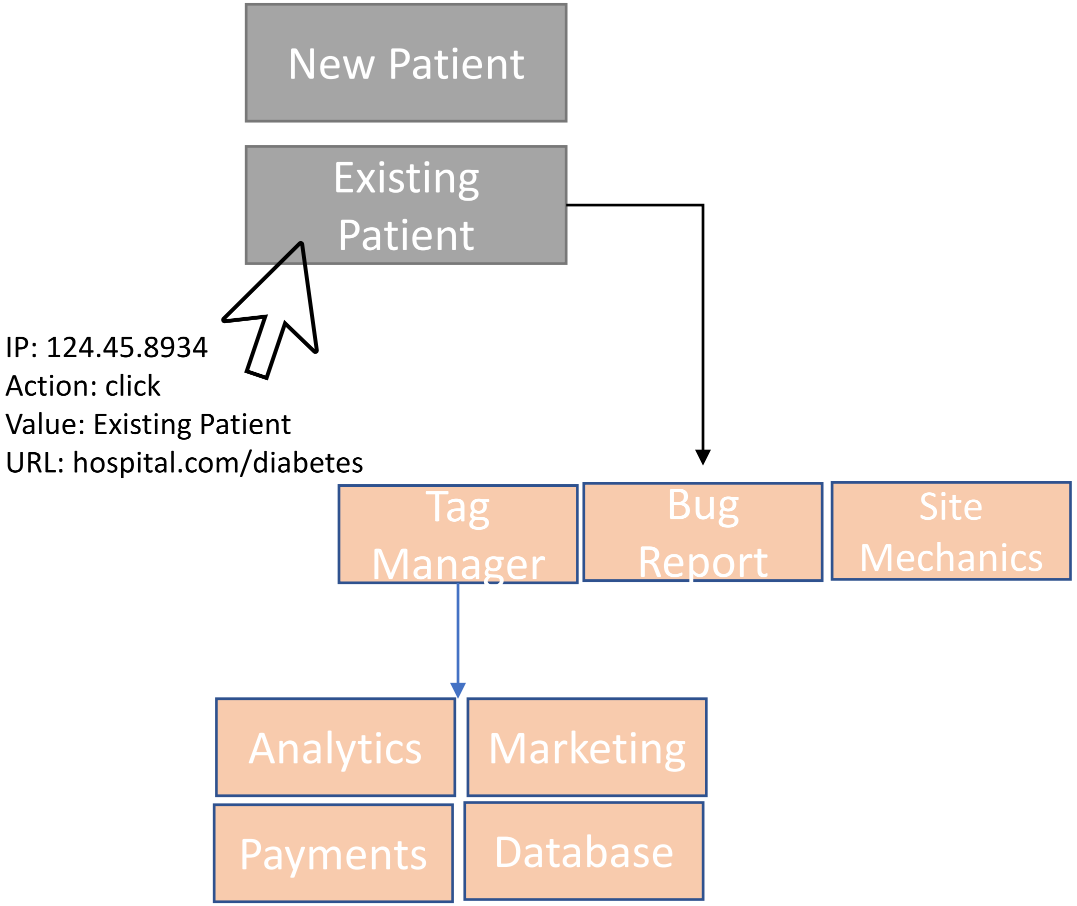


New Patient

Existing Patient

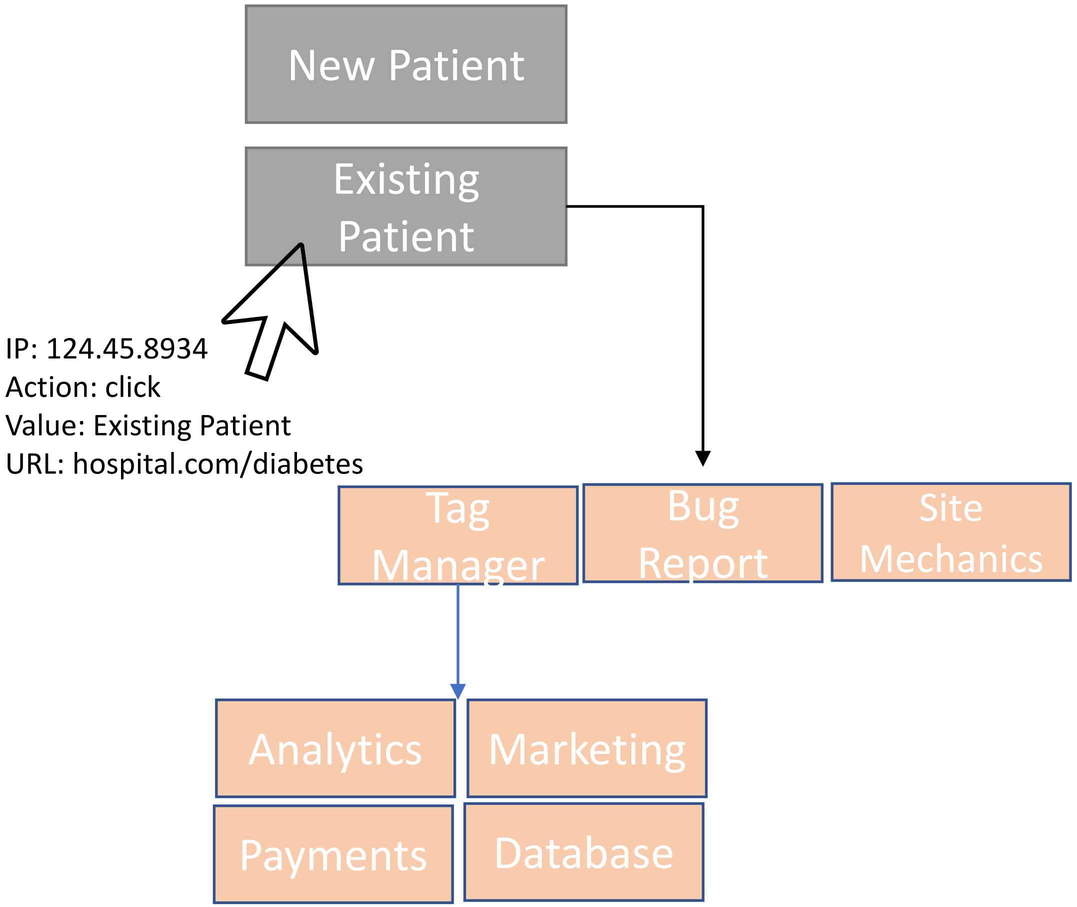
IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

What data gets sent where?



IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

What data gets sent where?

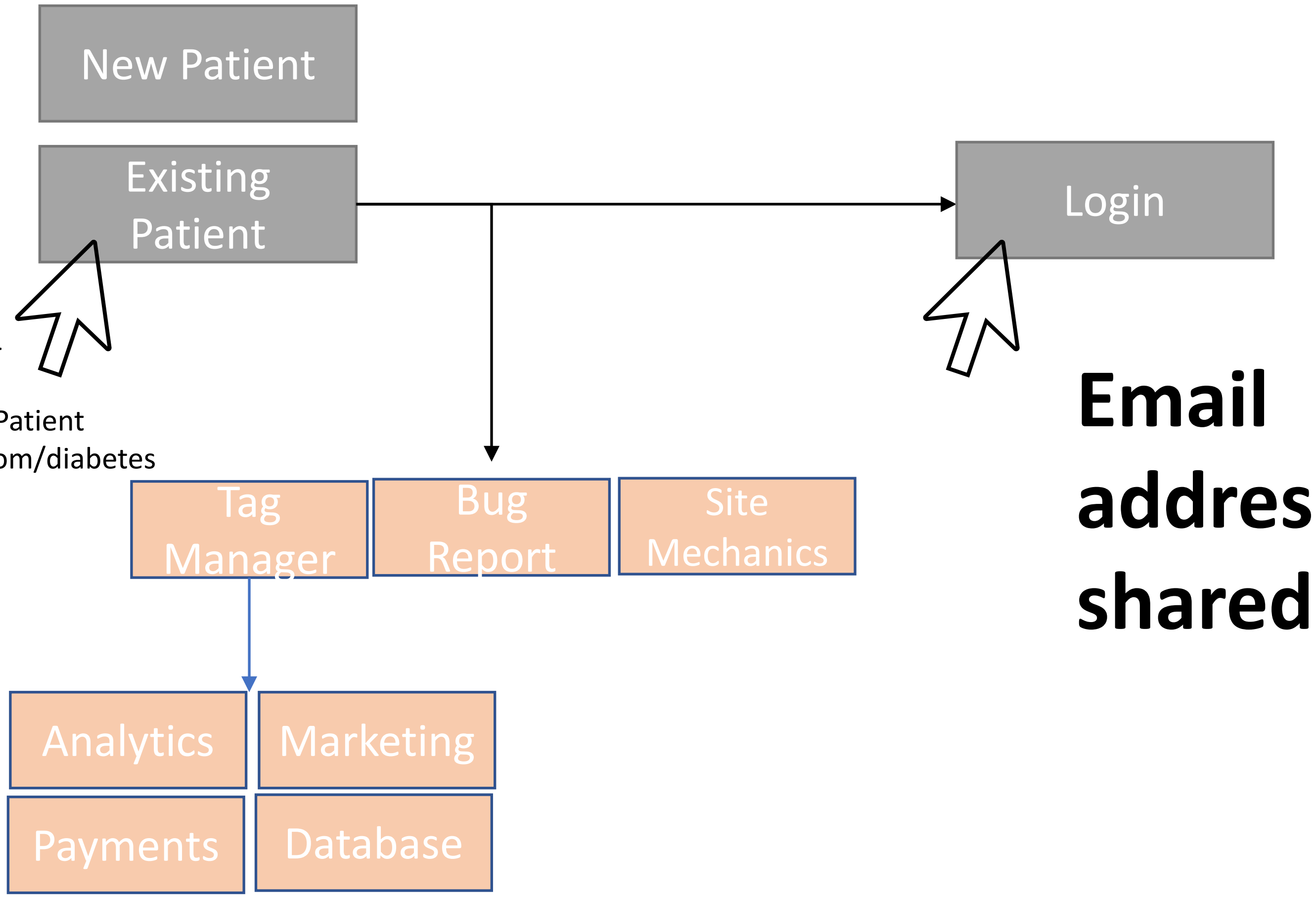


IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

BAAs?
Downstream use limitations?
Minimization?
Contractual prohibitions?

Who is the system owner?

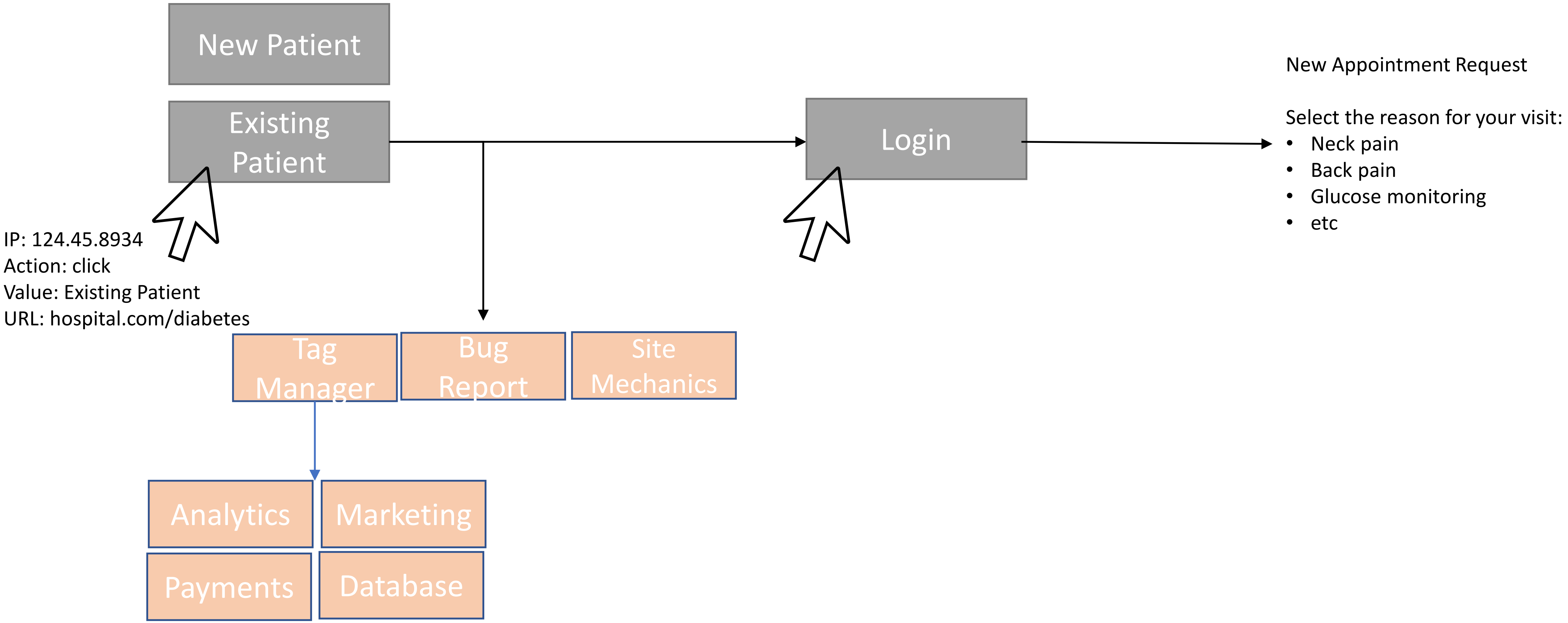
What data gets sent where?



IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

Email address shared?

What data gets sent where?



New Patient

Existing Patient

IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

Tag Manager

Bug Report

Site Mechanics

Analytics

Marketing

Payments

Database

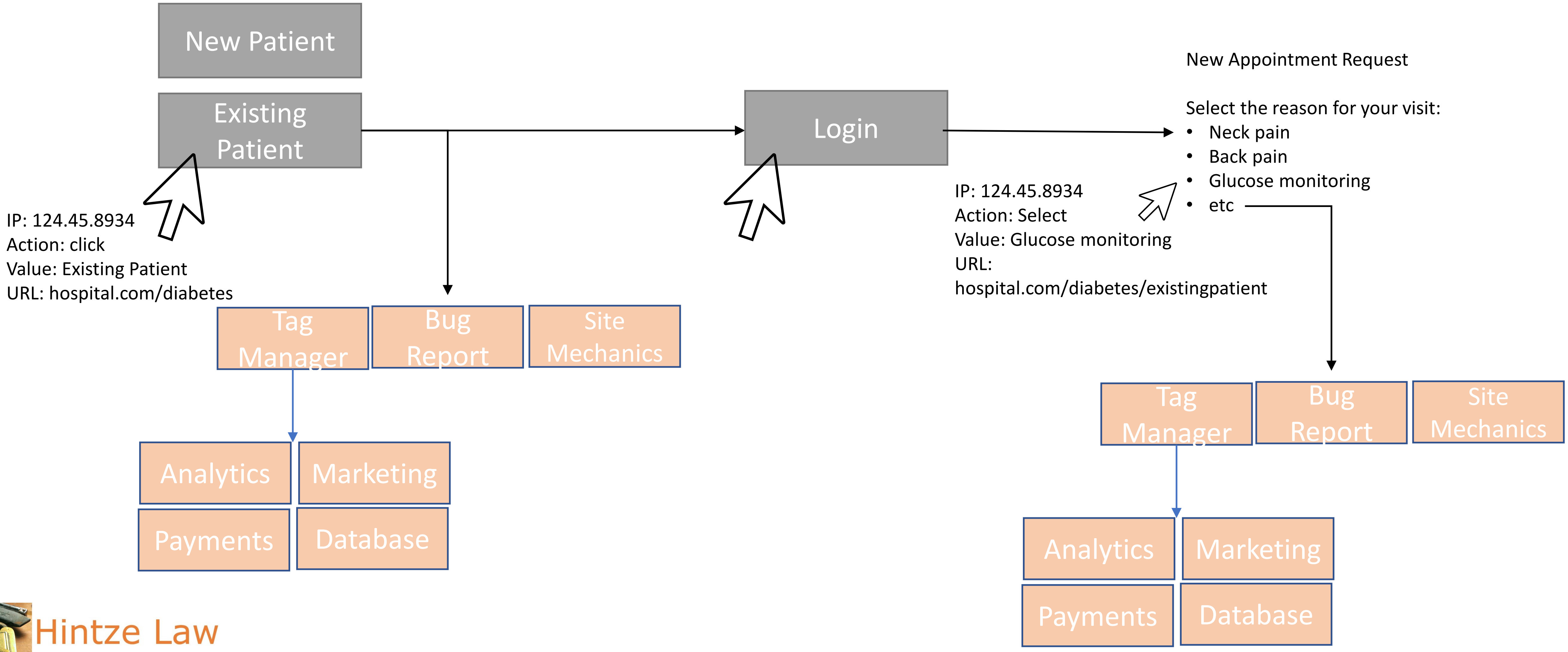
Login

New Appointment Request

Select the reason for your visit:

- Neck pain
- Back pain
- Glucose monitoring
- etc

What data gets sent where?



New Patient

Existing Patient

Login

IP: 124.45.8934
Action: click
Value: Existing Patient
URL: hospital.com/diabetes

Tag Manager

Bug Report

Site Mechanics

Analytics

Marketing

Payments

Database

New Appointment Request

Select the reason for your visit:

- Neck pain
- Back pain
- Glucose monitoring
- etc

IP: 124.45.8934
Action: Select
Value: Glucose monitoring
URL:
hospital.com/diabetes/existingpatient

Tag Manager

Bug Report

Site Mechanics

Analytics

Marketing

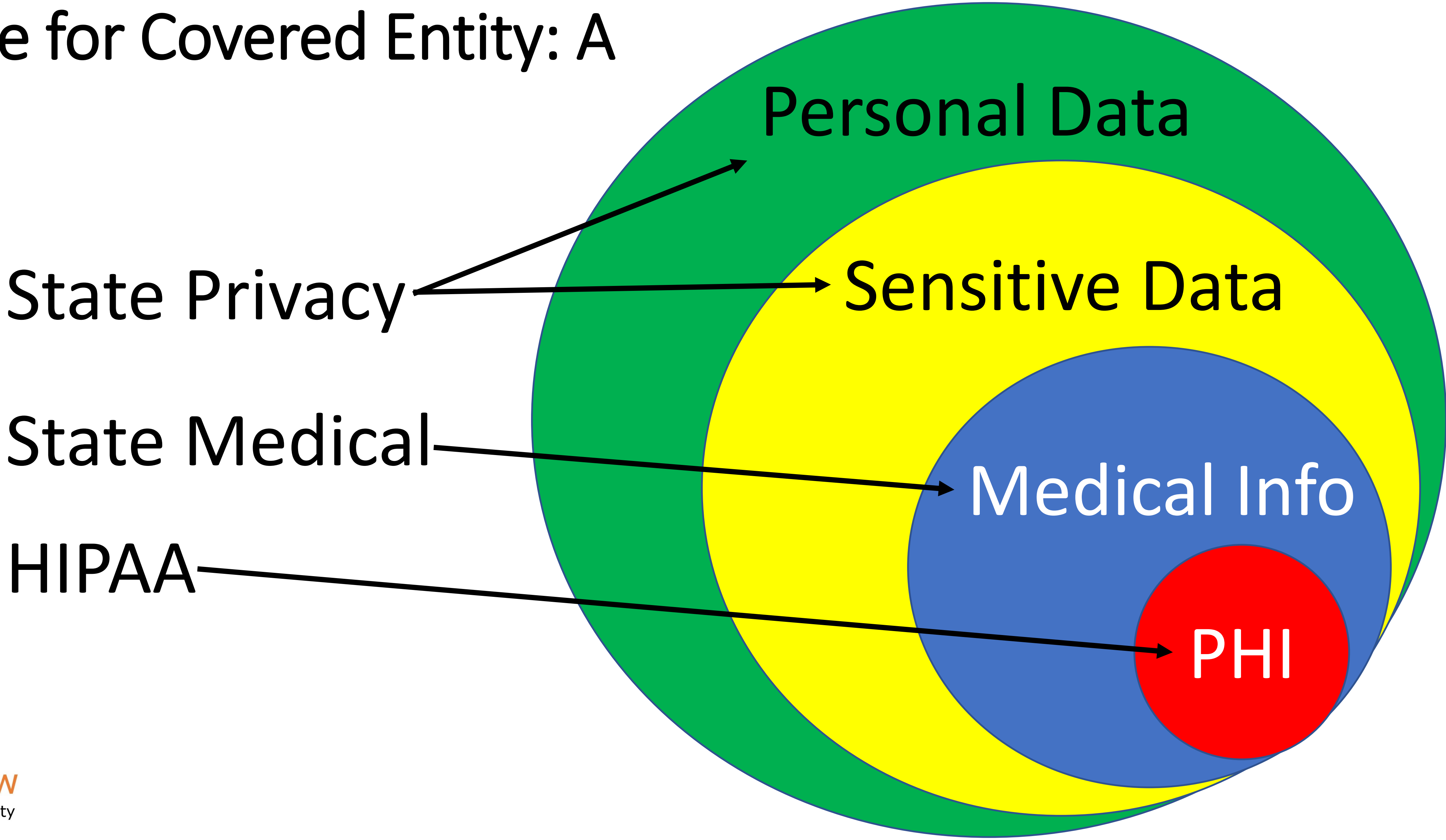
Payments

Database

The important lesson: “health” information can easily be exposed via existing tech infrastructure.

- Train your teams, especially back- and front-end engineers, data analytics, marketing, and product managers
- Develop data classification standards that are clear, accessible, and teach employees how to exercise judgment (or know when to ask for help)
- Privacy by design: don’t use health-related information in URLs, app events, etc.
- Likely cannot use out-of-the-box tracking solutions that use javascript

Possible Regulatory Scheme for Covered Entity: A Mess!



State Privacy

State Medical

HIPAA

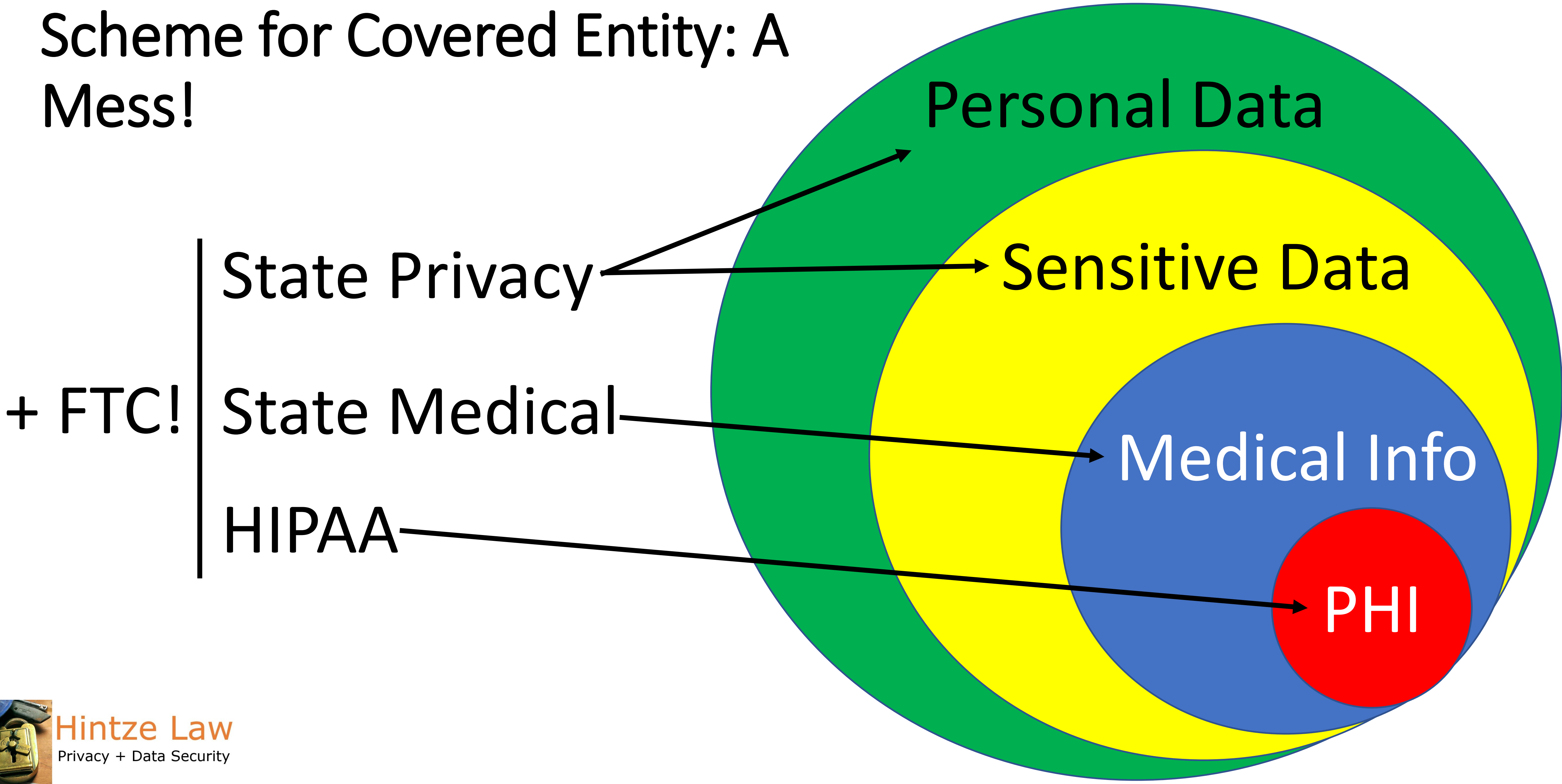
Personal Data

Sensitive Data

Medical Info

PHI

Possible Regulatory Scheme for Covered Entity: A Mess!



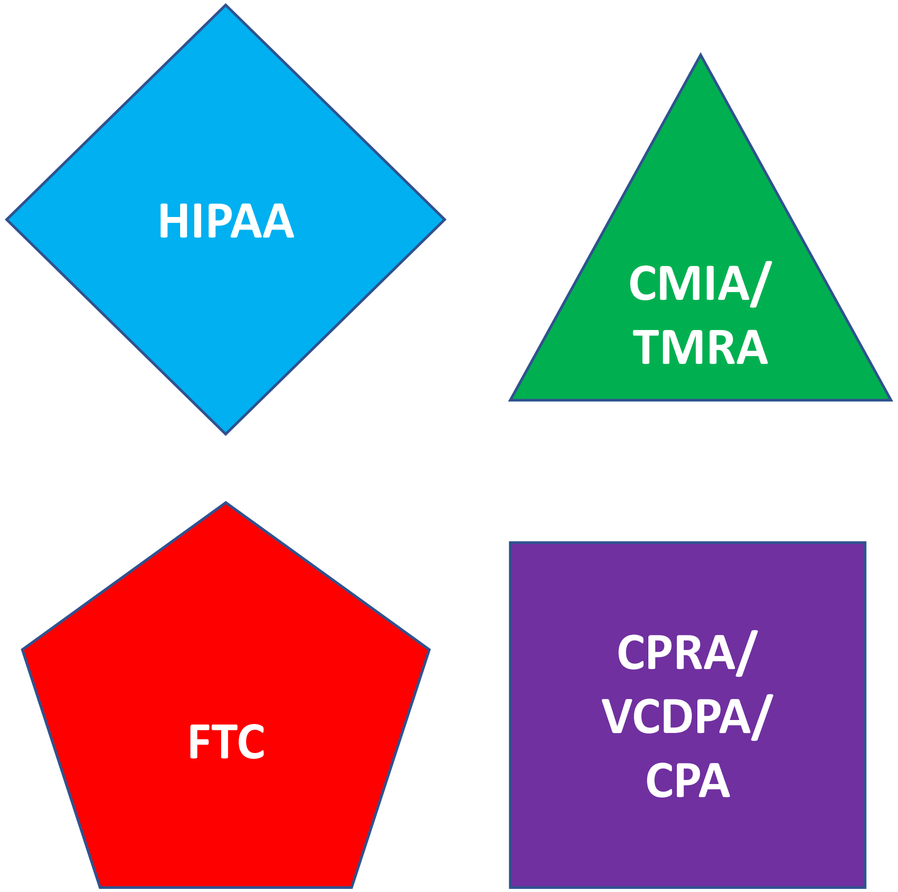
+ FTC!

State Privacy

State Medical

HIPAA

The bucket that health data falls into can change based on context.



HIPAA

CMIA/ TMRA

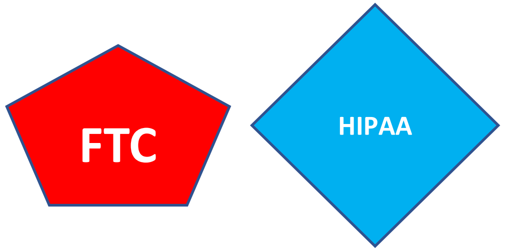
FTC

CPRA/ VCDPA/ CPA

Where does it fit?

Health Info

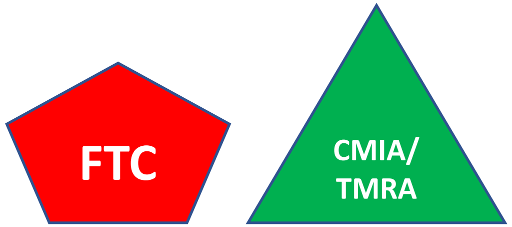
The bucket that health data falls into can change based on context.



FTC

HIPAA

A medical provider diagnoses a patient with diabetes. This information is PHI with respect to the provider and their BAs. The provider is also subject to FTC unfair/deceptive enforcement.



FTC

CMIA/ TMRA

The patient uses an app on their phone to keep track of their health. They include their diabetes diagnosis in the app. The app is a “provider” under CMIA and covered by the FTC’s Health Breach Notification Rule.

CPRA etc

The patient joins diabetes support groups online; record of this is likely sensitive information under CPRA/VCDPA/CPA.

A few other laws to consider…

- Part 2 Regulations (substance abuse)
- Common Rule (research)
- Fair Credit Reporting Act (reporting to credit agencies)
- Family Educational Rights and Privacy Act (school health records)
- Gramm-Leach-Bliley Act (insurance underwriting)
- Genetic Information Nondiscrimination Act (genetic privacy)
- Telephone Consumer Protection Act (communicating with patients)
- HIV Privacy Laws
- Mental Health Privacy Laws
- State Medical Record Access

Q&A

mason@hintzelaw.com

6th Annual Technology and Justice for All CLE

December 2, 2022

Texas Law Center, 1414 Colorado St, Austin, TX

SESSIONS:

- Technology Bootcamp for Attorneys
- Cyber Insurance / Cyber Due Diligence
- HR & Cybersercurity / Courtroom Tech
- 30 Apps in 30 Minutes / Space Law

https://statebaroftexassections.redpodium.com/cts2022cle

Computer & Technology Section Members: $125

Section Non-Members: $150 (includes membership)

COMPUTER AND TECHNOLOGY SECTION