Open@Epic CONFERENCE 2025

Regulation and Responsibility

US Law's Impact on Data Security and Privacy

Presenters

Daniel Gottlieb

McDermott, Will & Schulte

Patrick Harrigan

Epic

Disclaimer

- We aren’t your lawyers and none of this is legal advice.
- You should consult your own attorneys for legal advice.
- Daniel represents Epic customers and developers that integrate with Epic software. He is not Epic’s counsel.

Learning Objectives

1. Get a sense of the breadth of federal and state laws that might impact developers of health apps.
2. Hear about recent trends from enforcement and litigation in the data privacy space.
3. Learn practical questions to ask when implementing compliance plans.

Agenda

01 Consumer Data Use and Privacy Landscape

02 HIPAA and Data Breach

03 Privacy Litigation Risks and Landscape

04 Information Blocking

05 Practical Take Home

Patient Data Use and Privacy Landscape

Patchwork Quilt of Laws

General Health Privacy Laws

- HIPAA
- California CMIA

State Consumer Health Privacy

- WA My Health My Data Act

Consumer Protection Laws

- FTC Act section 5
- State unfair and deceptive practices

Sensitive Health Information Laws

- California CMIA
- 42 CFR Part 2

State Personal Information Privacy

- CA Consumer Privacy Act
- TX Data Privacy & Security Act

State Reasonable Security Practices

- Mass. Gen. Law ch. 93H
- New York SHIELD Act

Who are the developer's customers?

What data is the app collecting?

Where is the app conducting business?

Who's Who? The Enforcers

HHS Office for Civil Rights

Enforces HIPAA and 42 CFR Part 2

Jurisdiction over Covered Entities and BAs.

State Attorneys General

Can enforce HIPAA & state consumer protection & data privacy laws.

Federal Trade Commission

Enforces FTC Act (including section 5) and other federal antitrust laws.

Private Plaintiffs

Can sue for statutory and actual damages (and atty fees) under some state laws. Some laws allow class actions.

Who's Who? The Enforcers

HHS Office for Civil Rights

Enforces HIPAA and 42 CFR Part 2

Jurisdiction over Covered Entities and BAs.

State Attorneys General

Can enforce HIPAA & state consumer protection & data privacy laws.

Federal Trade Commission

Enforces FTC Act (including section 5) and other federal antitrust laws.

Private Plaintiffs

Can sue for statutory and actual damages (and atty fees) under some state laws. Some laws allow class actions.

Who's Who? The Enforcers

HHS Office for Civil Rights

Enforces HIPAA and 42 CFR Part 2

Jurisdiction over Covered Entities and BAs.

State Attorneys General

Can enforce HIPAA & state consumer protection & data privacy laws.

Federal Trade Commission

Enforces FTC Act (including section 5) and other federal antitrust laws.

Private Plaintiffs

Can sue for statutory and actual damages (and atty fees) under some state laws. Some laws allow class actions.

Who's Who? The Enforcers

HHS Office for Civil Rights

Enforces HIPAA and 42 CFR Part 2

Jurisdiction over Covered Entities and BAs.

State Attorneys General

Can enforce HIPAA & state consumer protection & data privacy laws.

Federal Trade Commission

Enforces FTC Act (including section 5) and other federal antitrust laws.

Private Plaintiffs

Can sue for statutory and actual damages (and atty fees) under some state laws. Some laws allow class actions.

Federal Enforcement Trends

OCR

Focus on HIPAA patient right of access and security risk assessments

FTC

Online privacy policies, sensitive health information, information about children

Federal Enforcement Trends

OCR

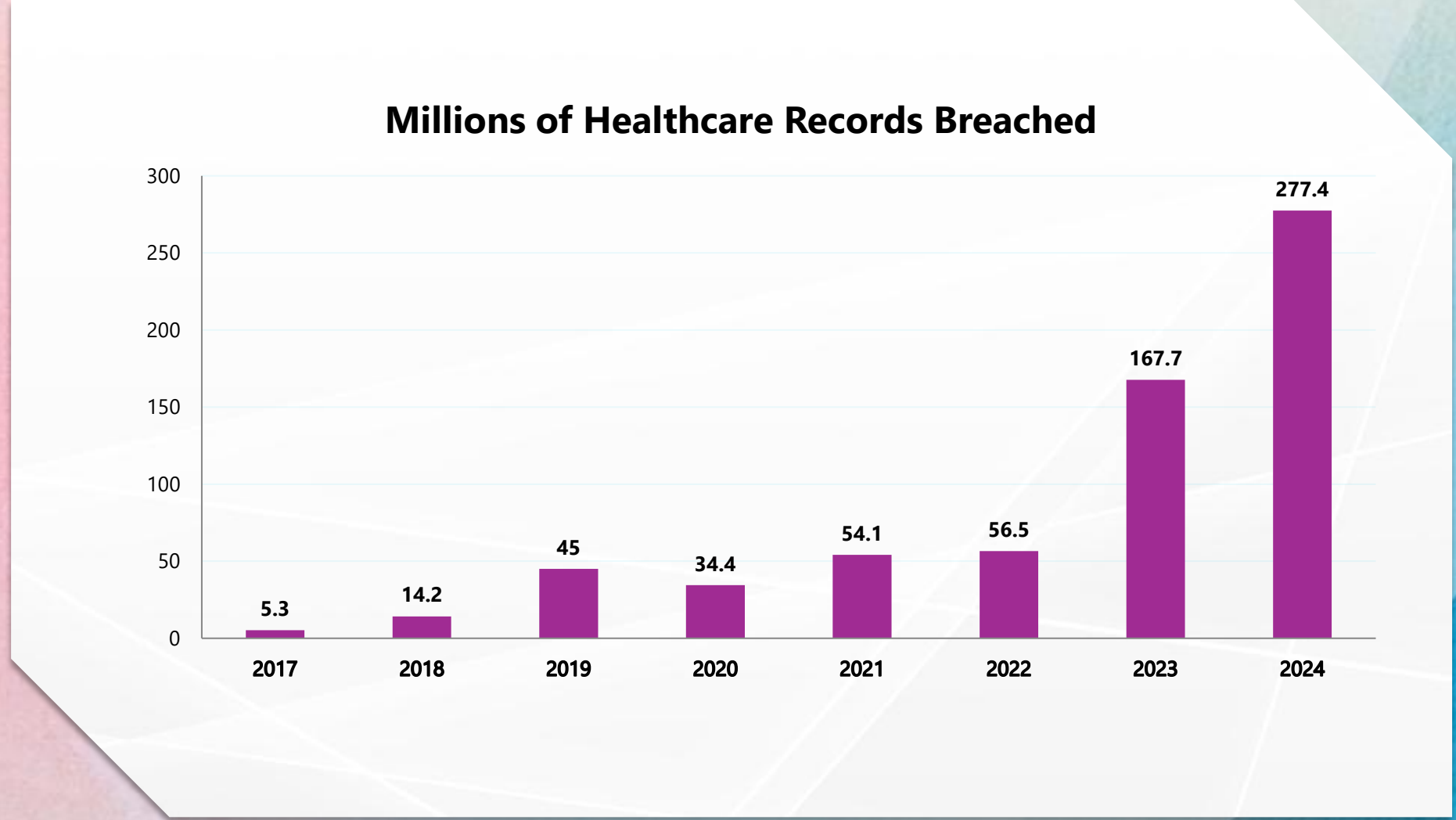
Focus on HIPAA patient right of access and security risk assessments

FTC

Online privacy policies, sensitive health information, information about children

HIPAA and Data Breach

Large Reported Breaches



Rise in Class Actions

Almost

1500

class actions

(2024)

Privacy Civil Litigation

Privacy Class Action Litigation

TCPA (Federal)

Requires consent for certain automated texts and calls

Statutory damages of $500 or $1500

Daniel's Law (NJ)

Prohibits disclosure of home address and phone # of law enforcement and judicial officers

$1000 for not taking down address or phone #

Biometrics (IL)

IL BIPA regulates collection and processing biometric info, requires consent for collection

Statutory damages ($1K or $5K)

Data Breach

Lots of legal theories: consumer protection law, negligence, breach of contract or fiduciary duty, etc.

Healthcare industry is big target

Tracking/AdTech

Claims based on old laws (federal and state wiretapping laws, VPPA, state privacy laws, etc.)

Healthcare industry is big target

Tracking/AdTech Technology

Claims based on old laws (wiretapping laws, VPPA, state privacy laws, etc.)

Healthcare industry is big target

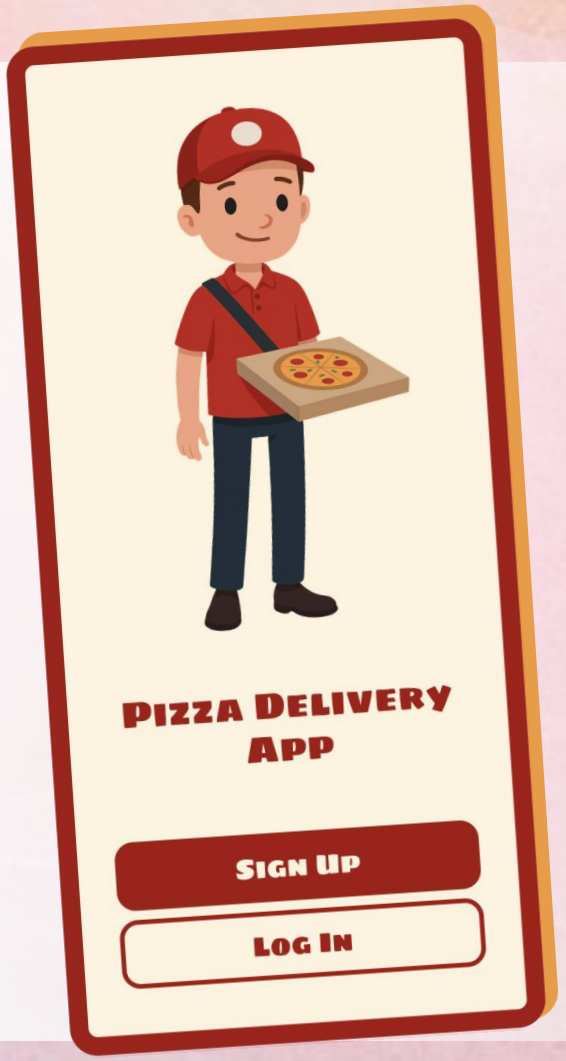
Civil Litigation Themes

- Embedded cookies
- Embedded “session replay” technologies
- Vendor-hosted chat bot software (including for “aiding and abetting”)
- Transmission of data in secure (e.g., PHI) portals.

HIPAA & Cookies

- OCR’s evolving guidance

AdTech Risk Checklist



- ❑ What tracking tech is deployed and where? (public website?)
- ❑ What type of data is being collected? (PHI? identifiable?)
- ❑ Is data being shared with third parties?
- ❑ How transparent are privacy policies & consent forms?
- ❑ Are the right agreements in place?

21st Century Cures Act and Information Blocking

Information Blocking: How We Got Here

2015

ONC report to Congress

2016

Congress passes Cures Act

Authorizes HHS to define "reasonable and necessary activities" and OIG penalties up to $1M

2019

ONC proposes Cures Rule

Defines EHI, actors, and creates exception-based framework with 8 exceptions

2020

ONC publishes Final Cures Rule

Adds Content & Manner exception

2021

Information Blocking Rule takes effect

2023

OIG Penalty Enforcement Begins

For developers, HIEs/HINs

2024

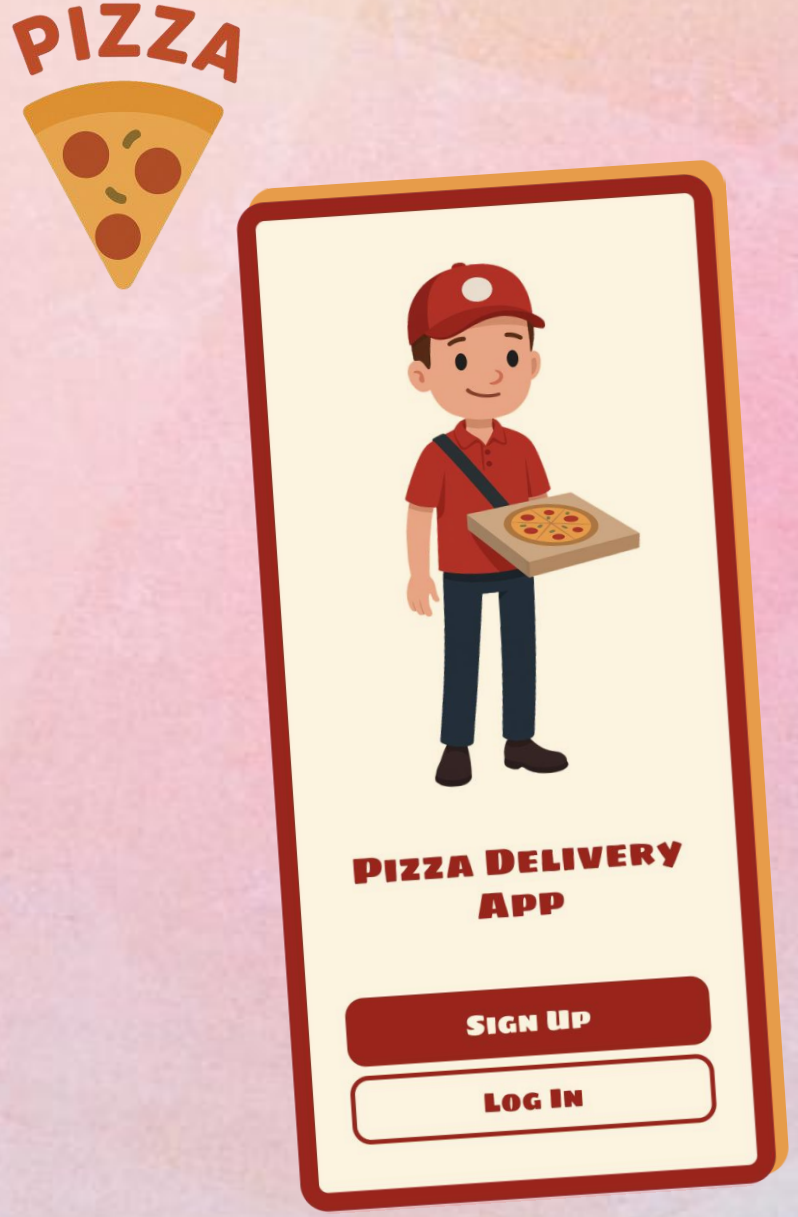
HTI-1, 2, and 3 released. CMS Disincentive Rule takes effect

Updated exceptions including TEFCA

2025

HHS priority

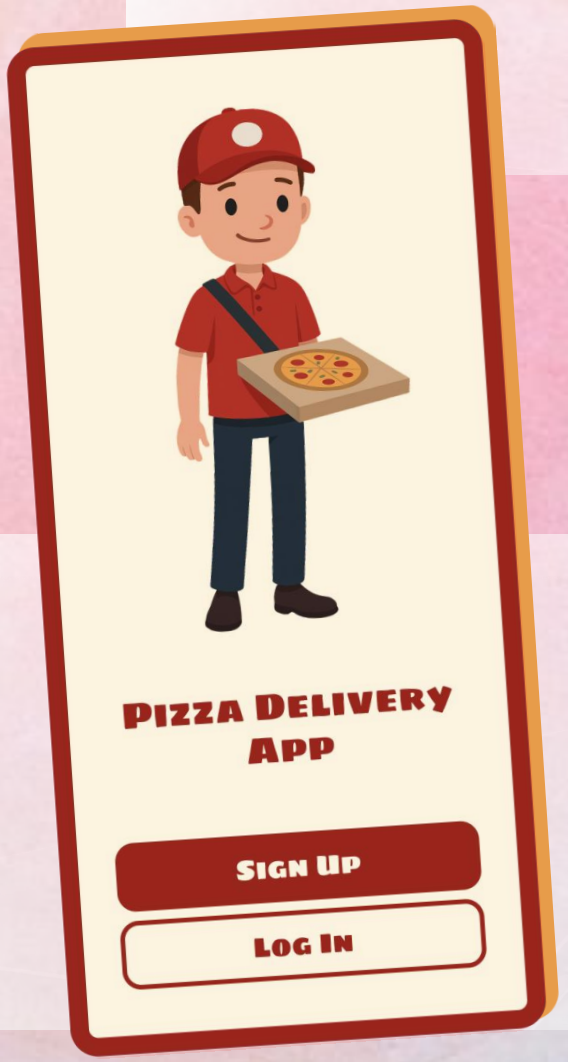
CMS RFI, ASTP bootcamp, OIG alert

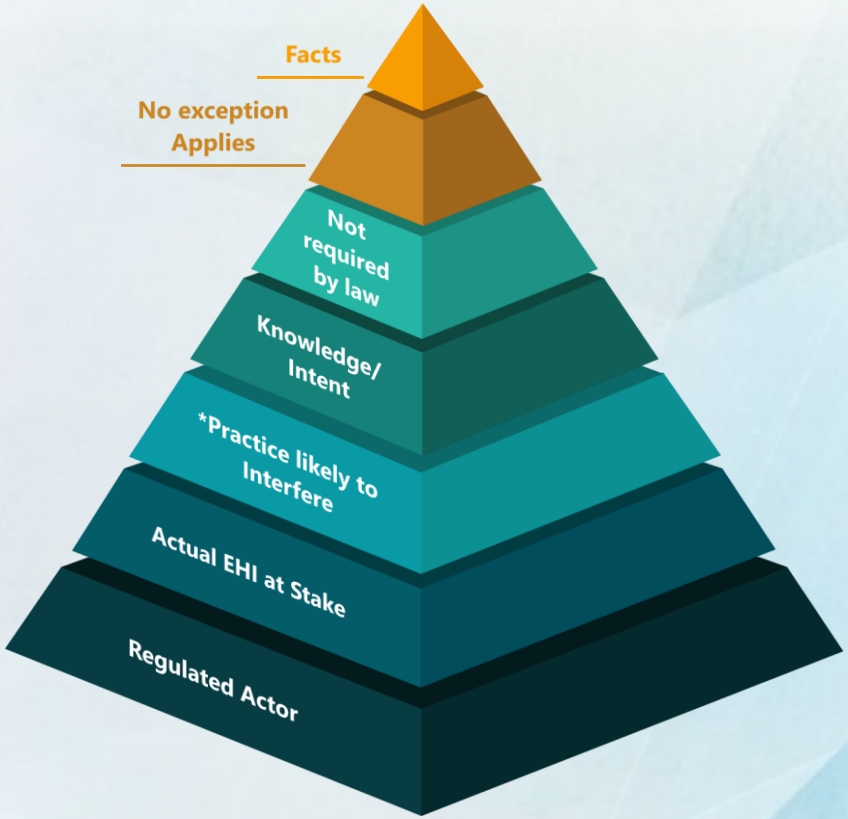


Scenario

- Pizza App partners with hospital so patients can order pizza from bedside and staff can order from break room and bedside
- Pizza app wants access to patient room number, demographics, allergies, and staff break room hours.
- Pizza app wants hospital IT staff to program a custom interface between its app and the hospital's instance of Epic. Hospital and app agree that app will pay actual costs plus reasonable margin

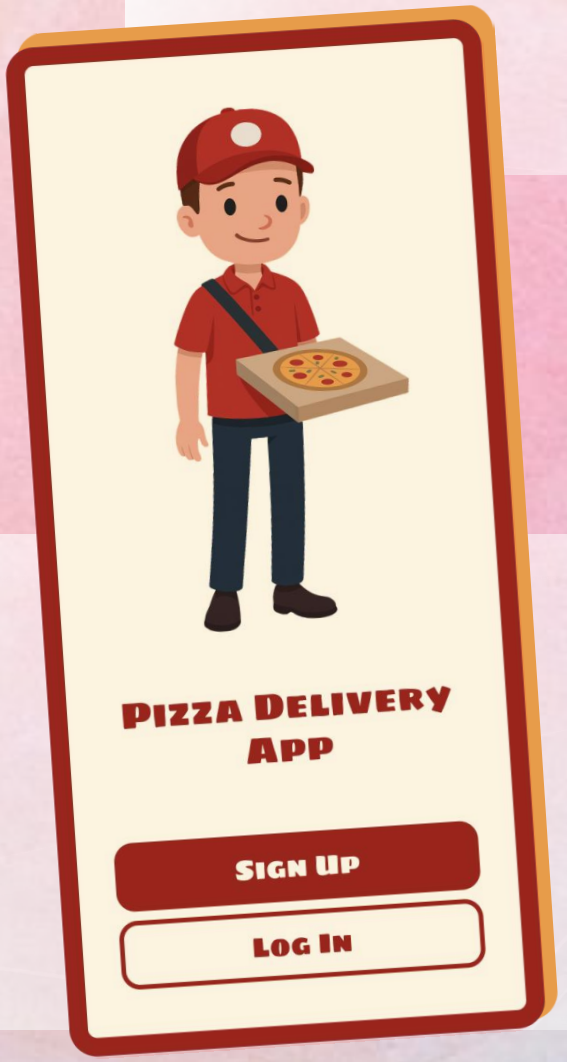
Scenario

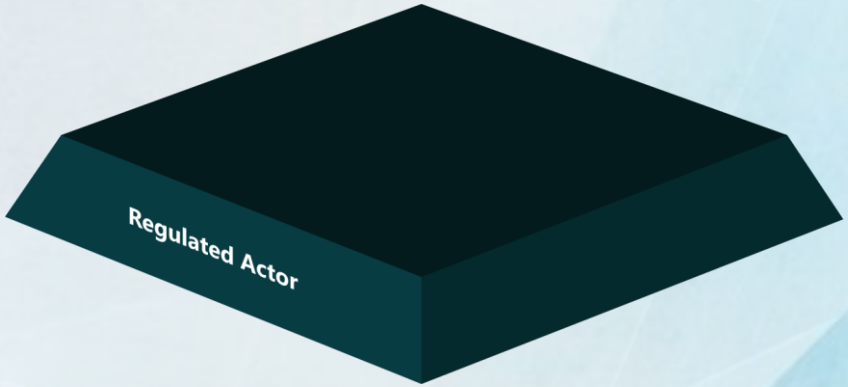




Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

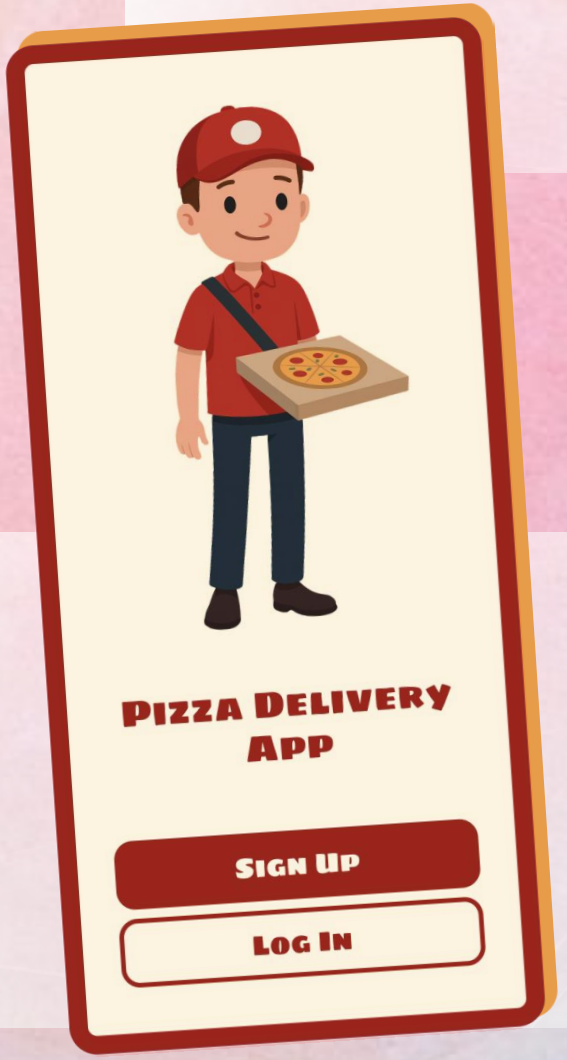
Scenario

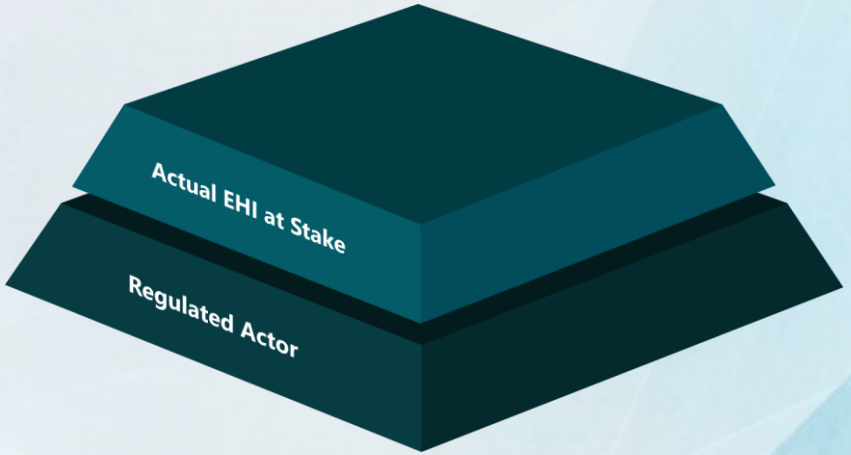




Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

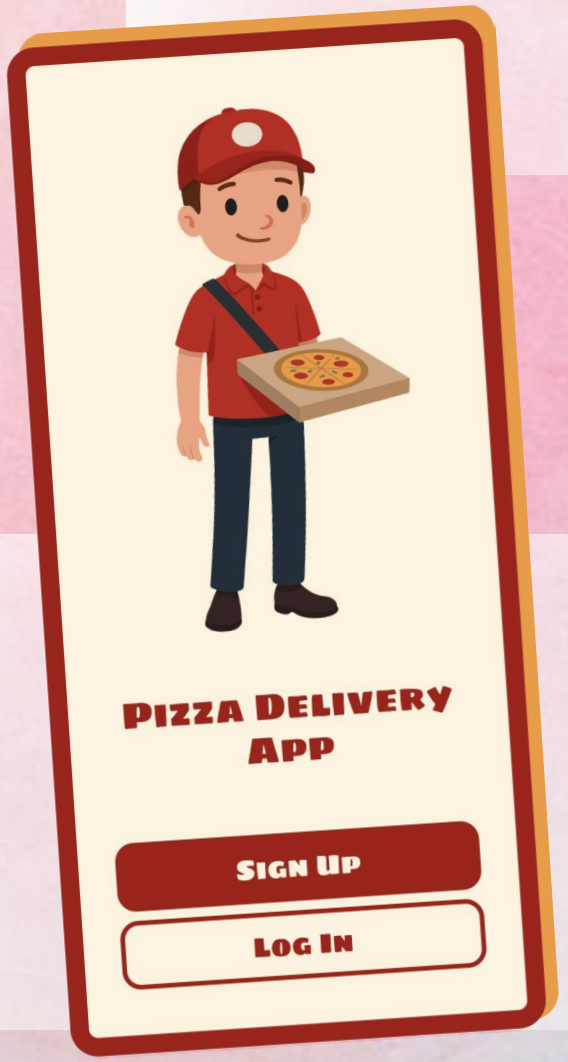
Scenario

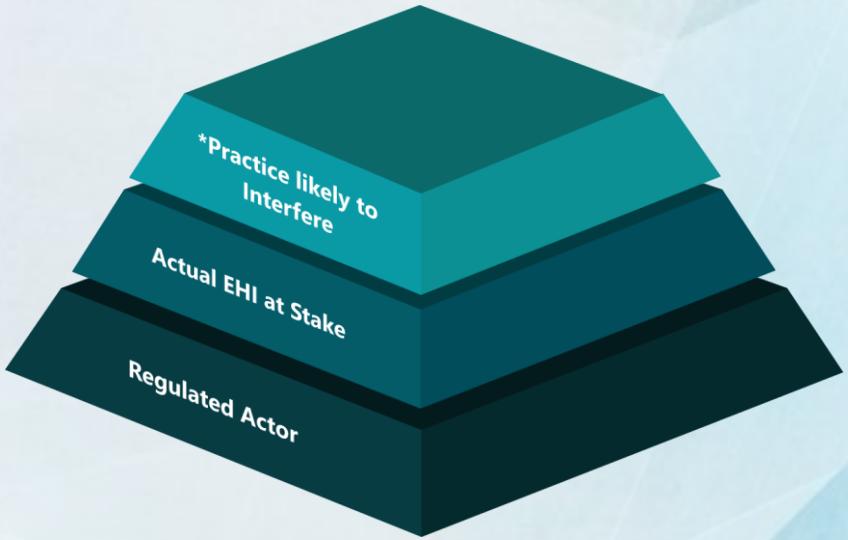




Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

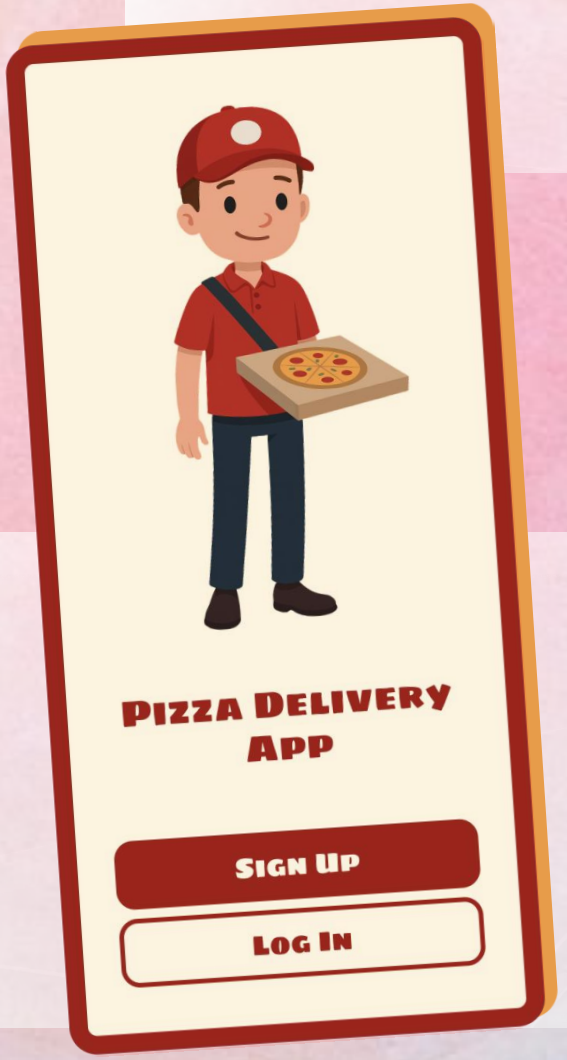
Scenario





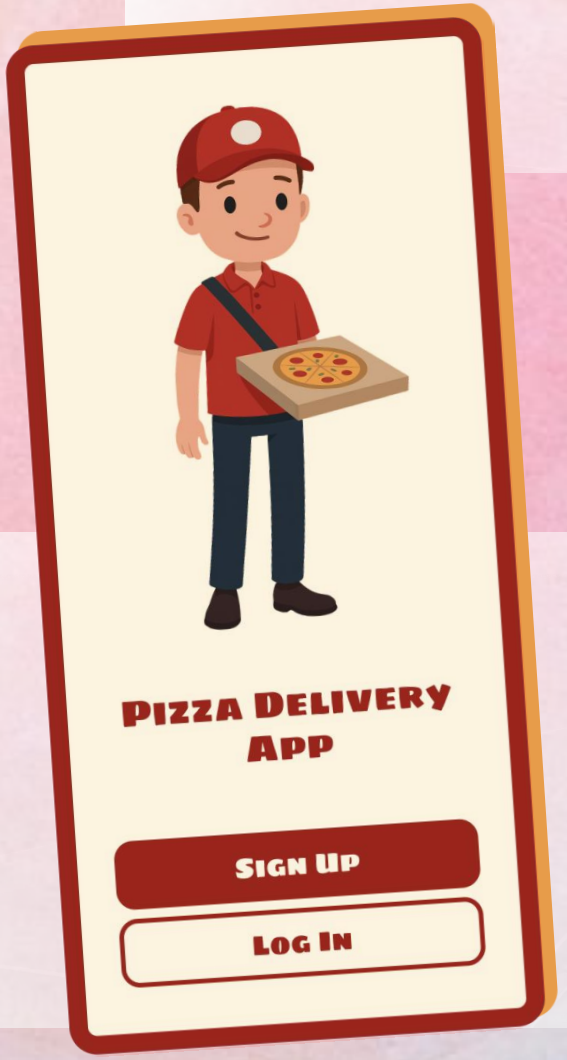
Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

Scenario



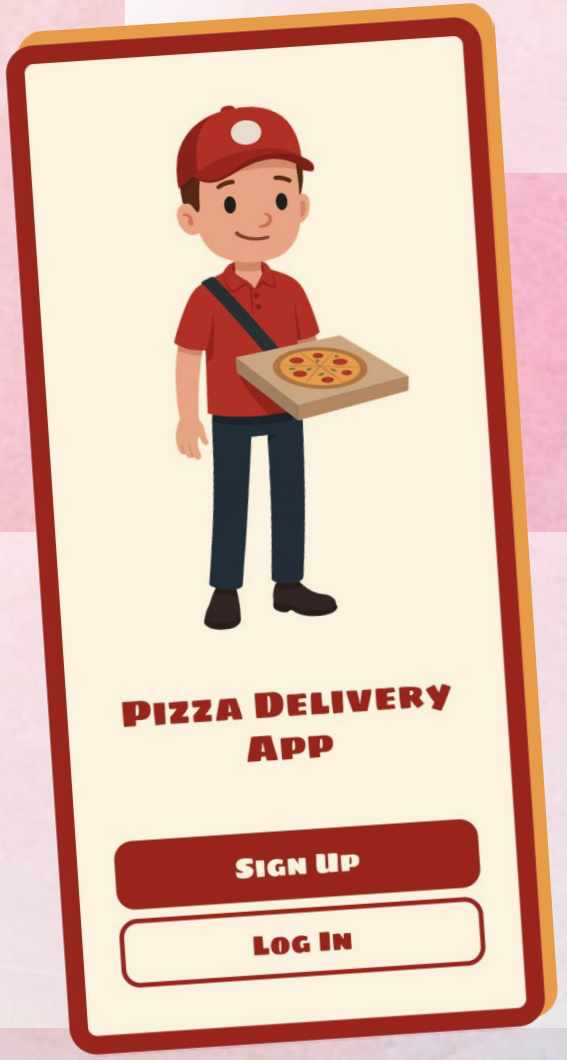
Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

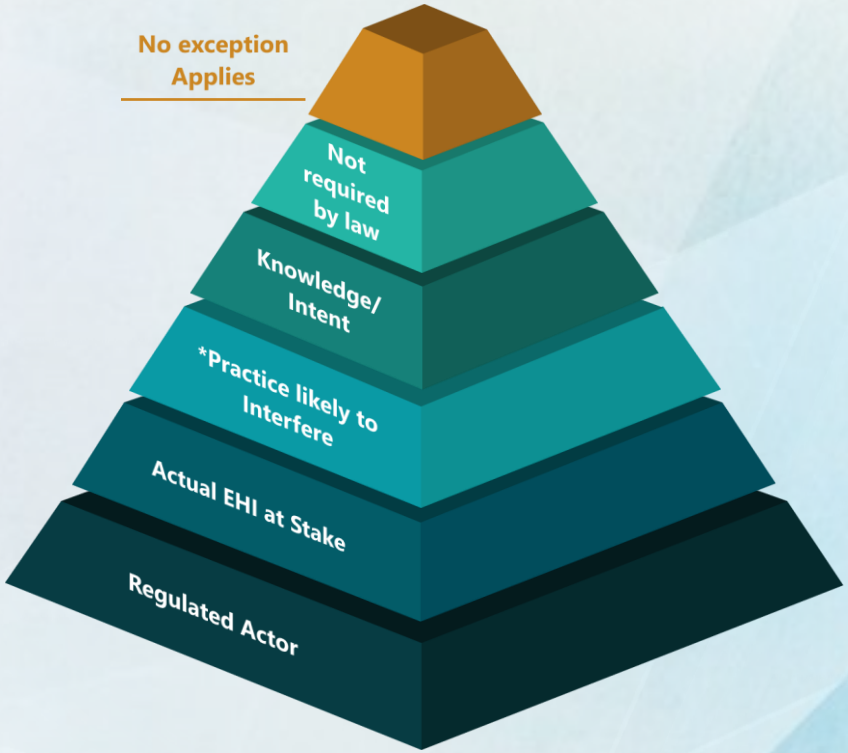
Scenario



Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

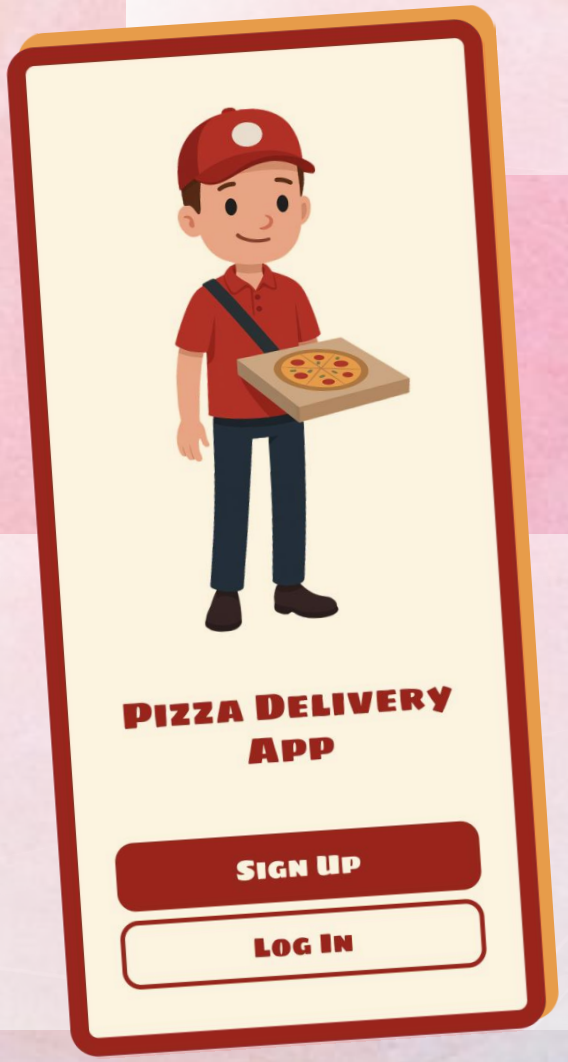
Scenario

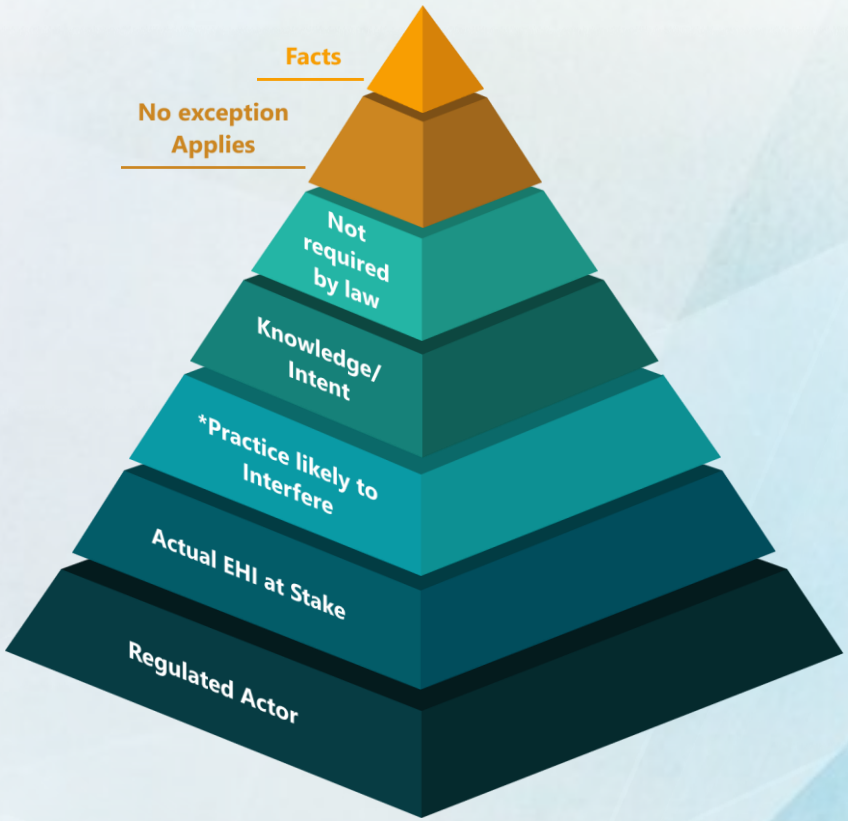




Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

Scenario





Sequoia Project
https://sequoiaproject.org/information-sharing-virtual-toolkit/

Take Home Tips

Data Handling

Avoid using **real patient data** in dev/test without approval and **encrypt** at rest and in transit.

Responsibilities

Confirm if you're a **Business Associate.** Look at **flowdown** obligations. Be ready for **audit.**

Security By Design

Apply **best consensus-based practices** like access controls, auditing and user tracking.

Secondary Use

De-identify PHI before reusing data for secondary purposes when required and as practical.

Transparency

Be transparent about **what** you collect, **why**, and **who** it's shared with in your patient/consumer-facing privacy policies.

Information Sharing

Focus on requests for **standards-based access** methods rather than bespoke requests when feasible.