Microsoft

BEYOND HIPAA

Regulating Data In the Health Sector

Trinity Car
Joanne Charles
Elliot Golding

MAY 26, 2021

Panelists

Trinity Car
Associate General Counsel & Privacy Officer
eHealth, Inc.

Joanne Charles
Principal Corporate Council
Microsoft

Elliot Golding
Partner
Squire Patton Boggs LLP

Legal disclaimer

The information contained in this presentation and delivered as part of this presentation are for educational and informational purposes only. The views, opinions and positions expressed by the panelists are theirs alone and do not necessarily reflect the views, opinions or positions of their employers, affiliated organizations or the Privacy + Security Forum.

Agenda

1. HIPAA & HITECH and Scope
2. Overview of Laws & Agencies Regulating Health Data
3. Use Cases & Analysis

HIPAA / HITECH

Health Insurance Portability and Accountability Act of 1996

Predates most modern online and mobile services and excludes health information created or managed by patients themselves.

Among other things, required the creation of national standards to protect the privacy and security of protected health information.

The Health Information Technology for Economic and Clinical Health Act (2009)

The focus of HITECH is on electronic health records (EHR). It was enacted in 2009 to cover the proposed increase in the use of electronic versions of PHI, aka ePHI.

The law is applicable to any organization that has set up an Electronic Health Record system.

What HIPAA does not cover

Data created or held by a person or company that is not a covered entity or business associate

Data that is collected and curated by consumers for their own use

Data that is not individually identifiable

Microsoft

Federal Laws
& Agencies Regulating Health Information

Existing Federal Privacy and Privacy-Related Laws
Potentially Applicable to Health Data

42 CFR, Part II Regulations:
Applies to patient information held by federally-funded substance abuse treatment programs

Federal Trade Commission Act:
Authority to address "unfair" or "deceptive" acts or practices in or affecting commerce related to health products

Family Educational Rights and Privacy Act (FERPA):
Applies to records maintained by education institutions related to student health as well as other educational records

And others…

Federal Authorities Regulating Health Data

Office of Civil Rights (OCR)	General Services Administration (GSA)	Substance Abuse and Mental Health Services Administration (SAMHSA)	Office of National Coordinator for Health Information Technology (ONC)
Food & Drug Administration (FDA)	Federal Trade Commission (FTC)	Office for Human Research Protections (OHRP)	
Centers for Disease Control & Prevention (CDC)		Office of the Inspector General (OIG)	Centers for Medicare and Medicaid Services (CMS)

For more information related to these agencies, please refer to our companion resource.

Microsoft

State Laws Regulating Health Information

Existing State Privacy and Privacy-Related Laws

Potentially Applicable to Health Data

State Breach Notification Laws

State Unfair or Deceptive Practices Statutes

California Consumer Privacy Act (CCPA)

Sector-Specific Regulations

And others...

State Authorities Protecting Health Data

State Courts	Medicaid		State Certifications
	Health Boards	Medical Boards	
Attorneys General		Licensure	State Pharmacy Board

For more information related to these agencies, please refer to our companion resource.

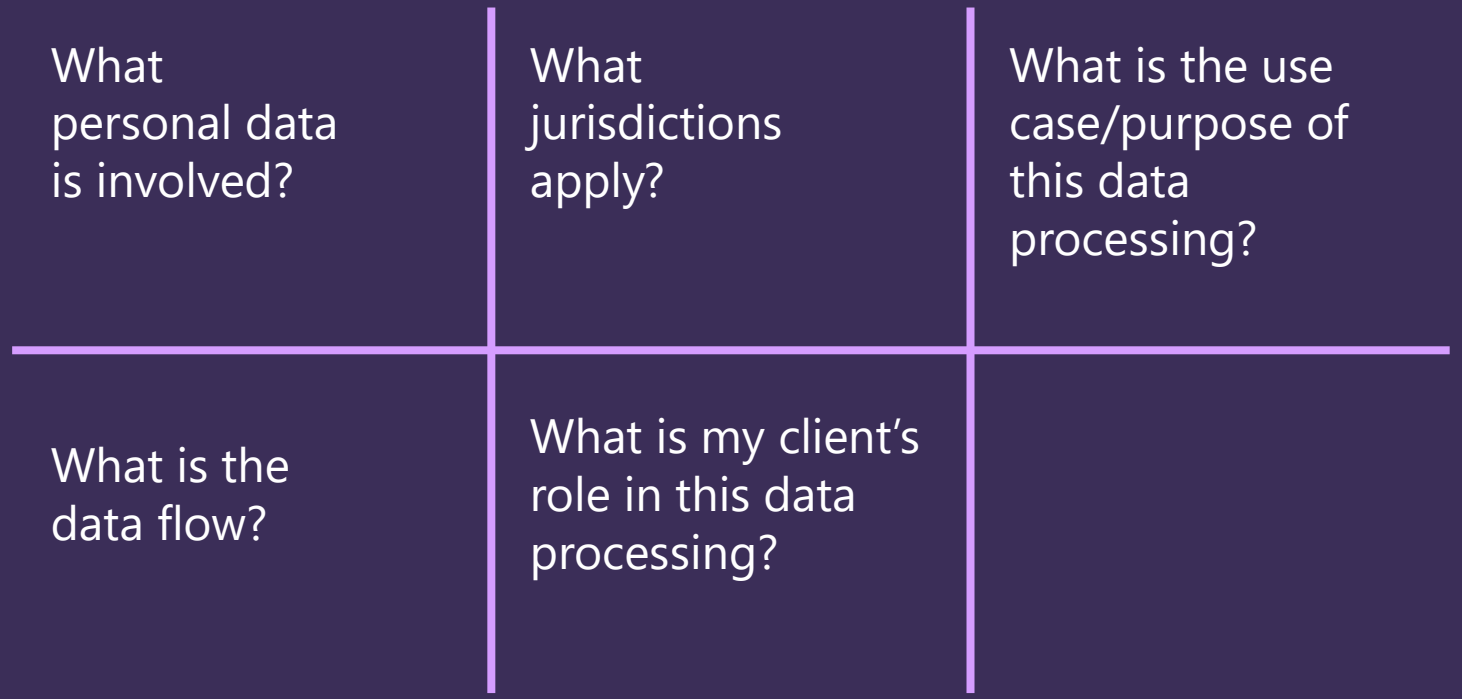
Microsoft

Use Cases & Analysis

Analysis Basics

Where to start?

What health privacy laws might apply?



Analysis Basics

Additional Considerations

What privacy policy applies and does this data processing align with the privacy policy?		What data retention requirements apply?
Has notice and consent been addressed?	What other stakeholders should be involved?	If working with another party, have you conducted privacy and security due diligence?
Does this health-related data require heightened security?	What will your press release say?	

Research / Data Analytics

Federal laws

The Federal Policy for the Protection of Human Subjects (Common Rule)

Section 5(a) FTC Act

Genetic Information Nondiscrimination Act (GINA)

State laws

California Consumer Privacy Act

Texas Medical Records Privacy Act

Virginia Consumer Data Protection Act

Issue spotting

Informed Consent

Authorization

Ethical Considerations

Sample Use Case >>>

A commercial property landlord is contacted by a health vendor (“WellDesk”). WellDesk will provide on-site kiosks to collect visitor information including name and address as well as information related to current age, weight and temperature; exposure to COVID-19 patients; and vaccine status.

The vendor can support the landlord’s desire to have a “Healthy Building” and will retain visitor personal and health information to develop health information analytics for proprietary software development.

Vulnerable Populations

Federal laws

Children's Online Privacy Protection Rule (COPPA)

Family Educational Rights and Privacy Act (FERPA)

42 CFR Part 2

State laws

State Laws governing "sensitive" conditions (e.g., SUD, mental health, genetic info, communicable disease)

State general privacy laws

Consent to treatment

Issue spotting

Consent Management

Role of Parties

Contracting

Accessibility/ Discrimination

Sample Use Case >>>

CareCo is a Residential Treatment Center (RTC) for adults and minors suffering from traumatic injuries as well as mental health issues, such as eating disorders and substance use disorders.

TeachIt is a start-up company that provides online educational courses. CareCo and TeachIt seek to partner to provide online courses to CareCo patients.

Advertising and Patient Communications

Federal laws

FTC—claims in advertisements and communications cannot be deceptive or unfair and must be evidence-based.

CAN-SPAM—governs the use of and requirements for commercial email

State laws

State UDAAP—claims in advertisements and communications cannot be deceptive or unfair and must be evidence-based.

DAA Self-Regulatory Principles*

Issue spotting

Ad Tech

Delivery Methods

Consent Management

Content Sensitivity

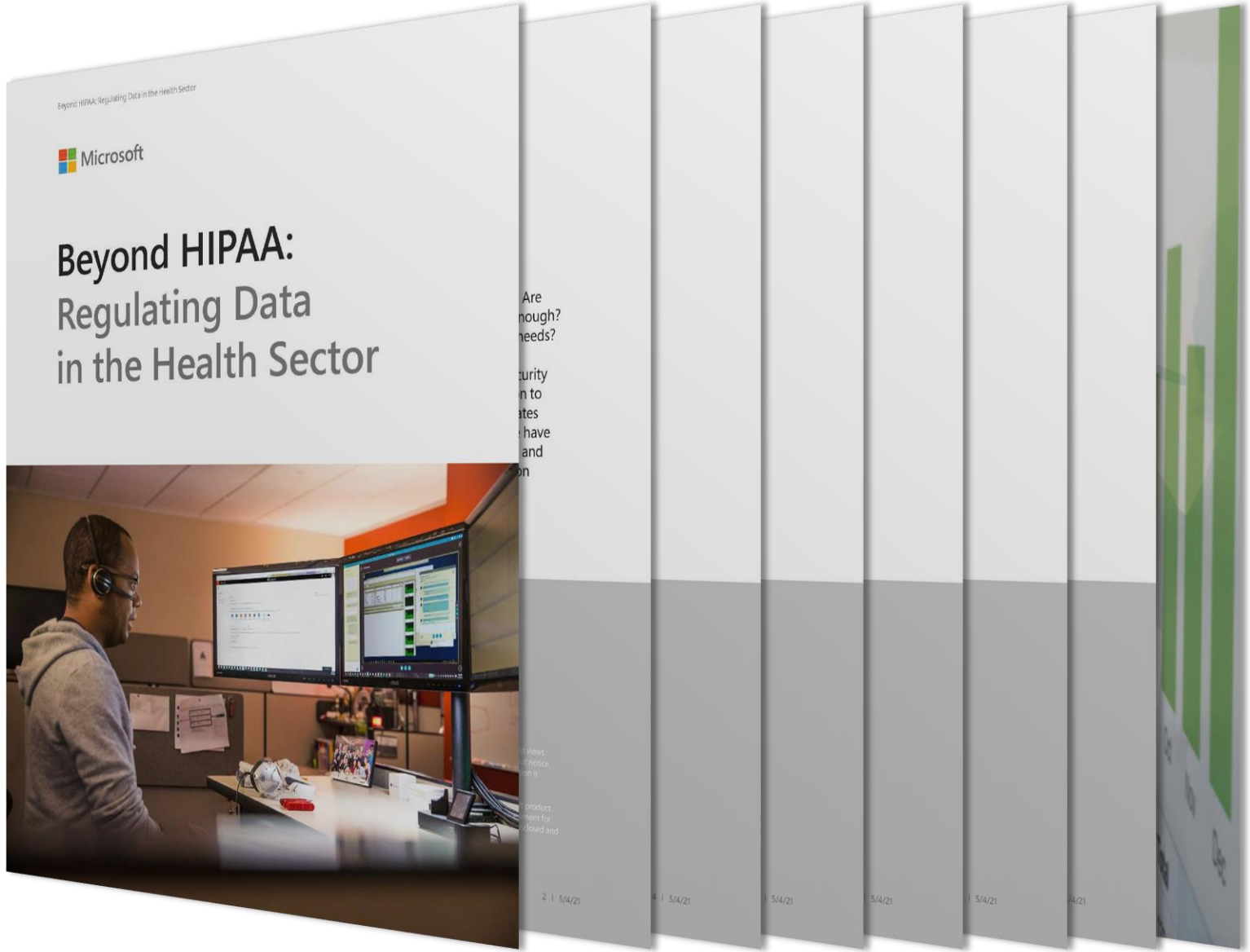
Sample Use Case >>>

A wearable exercise tracker, MoveIt, knows many of its customers have gained weight during the pandemic. MoveIt wants to partner with LoseIt, a weight-loss app, to provide these customers weight loss help and also create a new revenue stream for MoveIt.

Under the proposed partnership, MoveIt would share its customer PII (including name, age, address, email address, height, weight over time, bmi, exercise statistics, sleep statistics, average resting heart rate, and other health stats) with LoseIt, who would target its weight-loss app with an email campaign to MoveIt's customers who are over 18 and have gained 5+ pounds, have a BMI >25, or become less active over the last 12 months.

MoveIt would receive a payment for each MoveIt customer who becomes a LoseIt customer. LoseIt also wants to use the PII provided by MoveIt to build a new wellness-related product.

Resources



Download this here: https://tinyurl.com/2tn2xfjv