HEALTH PRIVACY
THE FTC PERSPECTIVE
2016 MATRC SUMMIT

Cora Han
April 12, 2016
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC

FTC Background

- Independent law enforcement agency
- Consumer protection and competition mandate
- Privacy is a consumer protection priority
  - Enforcement
  - Policy initiatives
  - Consumer education and business outreach

Area of FTC Focus

- Tremendous growth in consumer generated and controlled health data

WebMD

patientslikeme

HealthKit

- Much of this activity is taking place outside of HIPAA

Privacy and Security Challenges

- Security risks
- Risk of use and sharing of data in a way that consumers would not reasonably expect
- Increasing difficulty of defining health data
- Challenges of providing notice and choice

FTC Act Fundamentals

- Section 5 of the FTC Act broadly prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - **Deception**: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances
  - **Unfairness**: a practice that causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers

FTC Act Enforcement

- **PaymentsMD**
  - Medical billing company collected consumers' personal medical information without consent
- **GMR Transcription Services**
  - Medical transcription company outsourced services to third party without adequately checking to make sure they could implement reasonable security measures

Health Breach Notification Rule

- **Three types of covered entities**
  - Vendors of personal health records (PHRs)
  - PHR related entities
  - Third-party service providers

- **Requires covered entities that suffer a breach to:**
  - Notify everyone whose information was breached
  - In some cases, notify the media
  - Notify the FTC

Guidance for Mobile Health App Developers

- Interactive tool to help health app developers figure out which federal laws might apply to their app
  - Produced in cooperation with ONC, OCR, and FDA

Example – Dave's Wearable

- Is Dave's Activity Wearable from Scene #1 covered by HIPAA, the FTC Act, and/or the FD&C Act?

Guidance for Mobile Health App Developers

- FTC Best Practices
  - Minimize data
  - Limit access and permissions
  - Keep authentication in mind
  - Consider the mobile ecosystem
  - Implement security by design
  - Don’t reinvent the wheel
  - Innovate how you communicate with users
  - Don’t forget about other applicable laws

FTC Resources

www.ftc.gov www.business.ftc.gov

- Mobile Health App Developers
  - Interactive Tool
  - Best Practices
- Start with Security: A Guide for Business
- Careful Connections: Building Security in the Internet of Things
- Marketing Your Mobile App: Get It Right from the Start

Questions?

Cora T. Han
Federal Trade Commission
chan@ftc.gov