HEALTH INFORMATION PRIVACY AND SECURITY BEYOND HIPAA

NCVHS MEETING SEPTEMBER 13, 2017

Cora Han
Division of Privacy and Identity Protection
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
- Data security and privacy are consumer protection priorities
  - 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
- Section 5 authority extends to both HIPAA and non-HIPAA covered entities

FTC Act Enforcement

- **Henry Schein Practice Solutions, Inc.**
  - FTC alleged that provider of office management software for dental practices misrepresented that its software provided industry-standard encryption of sensitive patient information.
- **Practice Fusion**
  - FTC alleged that electronic health records provider misled consumers by failing to disclose adequately that physician reviews would be publicly posted.
- **Vizio**
  - FTC alleged that manufacturer of “smart” televisions misled consumers about its tracking of consumer viewing histories.

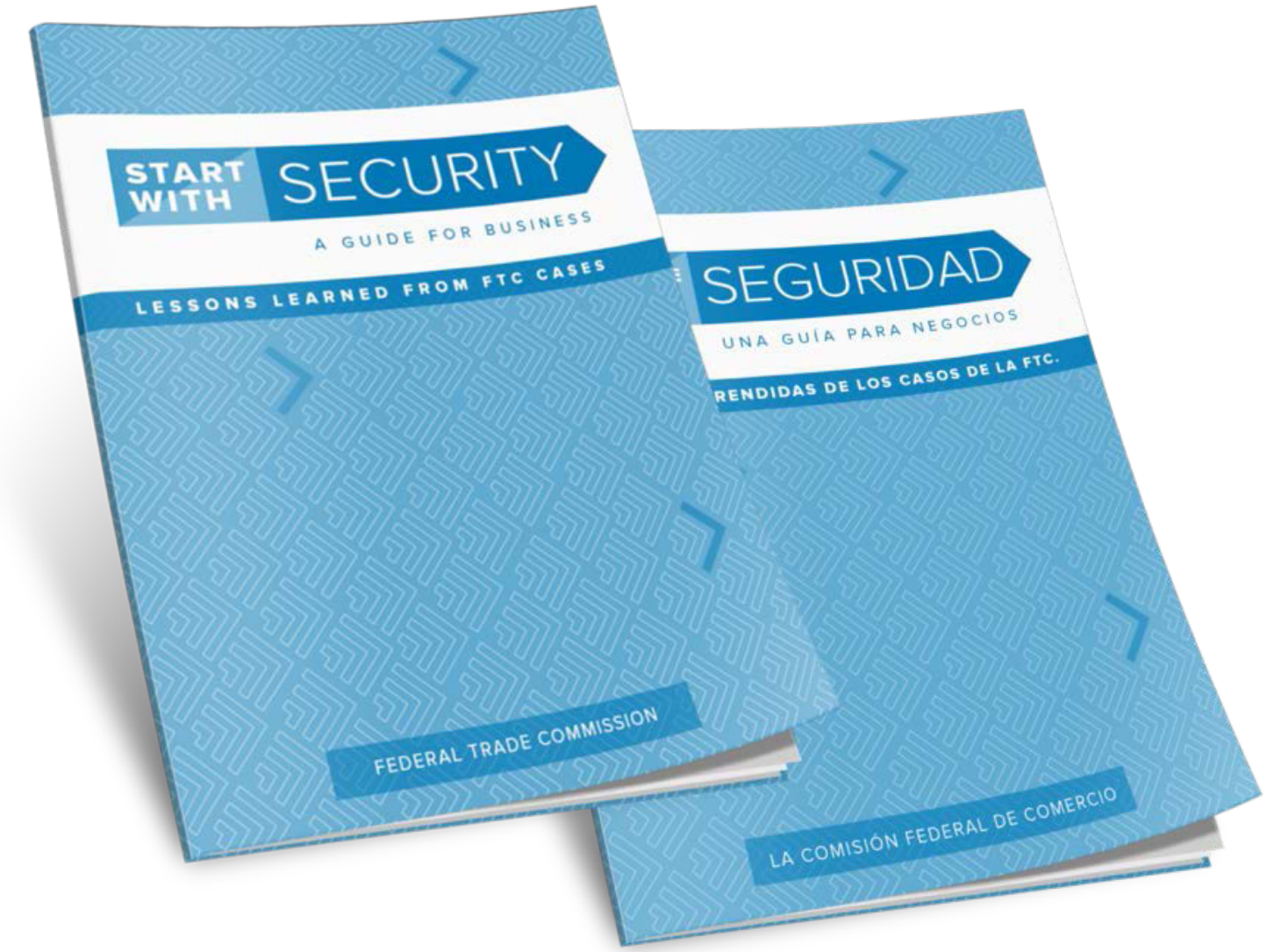
FTC Health Breach Notification Rule

- **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

***Does not apply to entities covered by HIPAA**

Start with Security



Start with Security: Best Practices

- Start with Security
- Control access to data sensibly
- Require secure passwords and authentication
- Store sensitive personal information securely and protect it during transmission
- Segment your network and monitor who’s trying to get in and out

Best Practices (cont.)

- Secure remote access to your network
- Apply sound security practices when developing new products
- Make sure your service providers implement reasonable security measures
- Put procedures in place to keep your security current and address vulnerabilities that may arise
- Secure paper, physical media, and devices

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

Produced in cooperation with the U.S. Department of Health & Human Services (HHS): the Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)

The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

FDA

Big Data Report

- Life cycle
- Benefits and risks
- Potentially applicable laws
- Research considerations

Benefits

- Increase educational attainment for individual students
- Provide access to credit using non-traditional methods
- Provide healthcare tailored to individual patients' characteristics
- Provide specialized healthcare to underserved communities
- Increase equal access to employment

Risks

- Result in more individuals mistakenly being denied opportunities based on the actions of others
- Create or reinforce existing disparities
- Expose sensitive information
- Assist in the targeting of vulnerable consumers for fraud
- Create new justifications for exclusion
- Result in higher-priced goods and services for lower income communities
- Weaken the effectiveness of consumer choice

Applicable Laws

- Fair Credit Reporting Act
  - Eligibility determinations
- Equal Credit Opportunity Act
  - Disparate treatment
  - Disparate impact
- Section 5 of FTC Act
  - Deceptive or unfair practices

Research Considerations

- Consider whether your data sets are missing information from particular populations and, if they are, take appropriate steps to address this problem.
- Review your data sets and algorithms to ensure that hidden biases are not having an unintended impact on certain populations.
- Remember that just because big data found a correlation, it does not necessarily mean that the correlation is meaningful. As such, you should balance the risks of using those results, especially where your policies could negatively affect certain populations.
- Consider whether fairness and ethical considerations advise against using big data in certain circumstances.

FTC Resources

www.ftc.gov

- Mobile Health App Developers
  - Interactive Tool
  - Best Practices
- Start with Security: A Guide for Business
- Big Data: A Tool for Inclusion or Exclusion?

Questions?

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