FTC HEALTH BREACH NOTIFICATION RULE

HIPAA Security Rule Conference, May 11, 2010

Cora Tung Han, FTC Division of Privacy and Identity Protection

BACKGROUND

- Part of the American Recovery and Reinvestment Act of 2009
- Interim final rule
- Enforcement began on February 22, 2010
- **Only applies to entities NOT covered by HIPAA**

WHO IS COVERED

- Vendors of personal health records (PHRs)
  - You are a **vendor of personal health records** if you offer or maintain a personal health record.

*A personal health record is an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

WHO IS COVERED

- PHR related entities
  - You are a **PHR related entity** if you
    - offer products or services through a website of a PHR vendor (even if the website is covered by HIPAA)
    - access information in a PHR; or
    - send information to a PHR

WHO IS COVERED

- Third-party service providers
  - You are a **third-party service provider** if you offer services to a PHR vendor or PHR related entity involving the use, maintenance, disclosure, or disposal of health information.

FAQ #1

- Our business is a HIPAA business associate. Does the FTC's rule apply to us?

WHAT TRIGGERS NOTIFICATION

- You must provide notice when there has been the **unauthorized acquisition** of **PHR-identifiable health information** that is **unsecured** and in a **personal health record**.

FAQ #2

- It looks like someone accessed our database without our consent. We don't know if they downloaded anything. Is this "unauthorized acquisition"?

FAQ #3

- We had a breach that affected only paper health records. Do we need to notify our consumers?

WHAT TO DO IF A BREACH OCCURS

- Who to Notify
  - If you are a PHR vendor or PHR related entity you must notify:
    - Affected persons
    - FTC
    - Under certain circumstances, the media
  - If you are a third-party service provider you must notify:
    - The PHR vendor or PHR related entity that is your client

WHAT TO DO IF A BREACH OCCURS

- When to notify
  - People
    - Without unreasonable delay and no later than 60 calendar days after the breach is discovered
  - FTC
    - More than 500 people = within 10 business days
    - Fewer than 500 people = annually
  - Media
    - For breaches that affect at least 500 residents of a particular state, the District of Columbia, or a U.S. territory or possession, without unreasonable delay and no later than 60 calendar days

WHAT TO DO IF A BREACH OCCURS

- How to notify people
  - By first-class mail or, if specified as a preference, by email
  - Substitute notice
    - Clear and conspicuous posting for 90 days on your home page, or
    - Notice in major print or broadcast media

WHAT TO DO IF A BREACH OCCURS

- What should the notice include
  - Brief description of what happened
  - Information involved in the breach
  - Suggested steps people can take to protect themselves
  - Steps you are taking to investigate the breach, protect against future breaches, and mitigate the harm from the breach
  - Contact information

FAQ #4

- What is the relationship between the FTC's Health Breach Notification Rule and state breach notification laws?

QUESTIONS?

www.ftc.gov/healthbreach