Notification for Breaches of Personal Health Records

Joint JCOTS and JCHC Study

October 7, 2009

Stephen W. Bowman
Senior Staff Attorney/Methodologist
Joint Commission on Health Care

Agenda

- Senate Bill 1229
- Virginia's Data Breach Law
- Federal Health Information Breach Notification Laws
- Joint JCOTS and JCHC Subcommittee Conclusions
- Policy Options

2

Senate Bill 1229 (Barker) was referred to JCOTS and JCHC for study

- Modifies Virginia's Database Breach Law to include notification for breaches of health information
  - Patron's intent - protecting health information not covered by Health Insurance Portability and Accountability Act (HIPAA)
  - Non-HIPAA covered entities with individually identifiable health information were **not** required to protect such information or notify when a breach occurred. Examples include:
    - Google Health
    - Microsoft Vault
    - Regional Health Information Organizations (RHIOs)
    - Other entities that collect personal health records

3

Virginia's Database Breach Law (2008)

- §18.2-186.6 of the *Code of Virginia* was adopted after four years of discussion and compromise. Entities involved:
  - Debt collection agencies,
  - Banking industry,
  - Consumer groups,
  - State Police, and
  - Other interested stakeholders.
- Law's purpose is to address instances of identity theft or other fraud

4

Virginia's Database Breach Law (2008)

"Personal information" is a person's first name or first initial and last name, in combination with one or more of the following:

1. Social Security Number
2. Driver's license number or state-issued ID number
3. Financial account number, credit card or debit card number, in combination with required security code, password, or access code
4. Medical information
5. Health insurance information

SB 1229 would add these

5

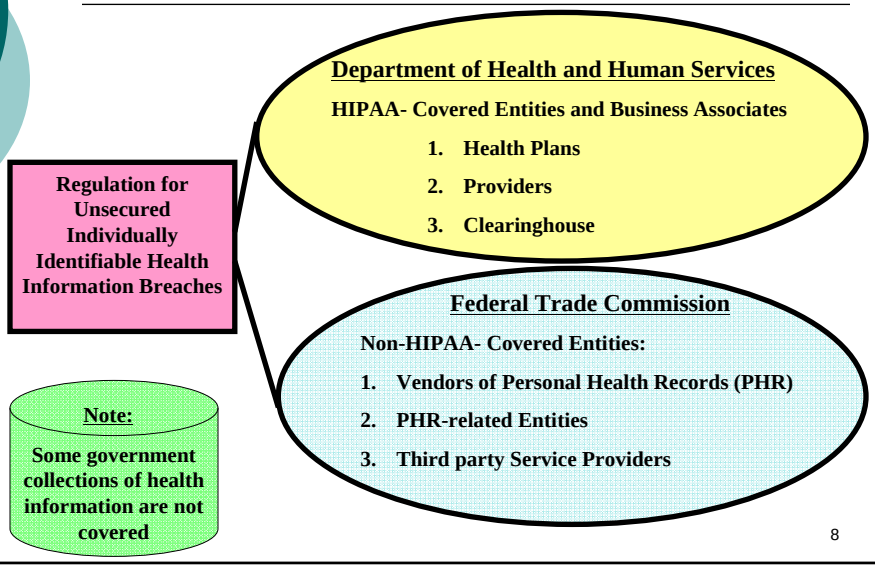
Recent Federal Health Information Protection Changes

HITECH Act Increase Health Information Protections

- HITECH Act passed February 17, 2009
  - Includes significant breach notification requirements for entities that have individually identifiable health information
  - Agencies that will promulgate regulations
    - Center for Medicare and Medicaid Services
    - Department of Health and Human Services (HHS)
    - Federal Trade Commission (FTC)
    - Office for Civil Rights

7

HHS and FTC Cover Entities that Possess Unsecured Individually Identifiable Health Information



8

Purpose of SB 1229 is Addressed by New FTC Regulations

- FTC regulations address non-HIPAA covered entities that collect personal health information, such as:
  - Examples of Vendors
    - Google Health
    - Microsoft Vault
    - RHIOs
  - Vendor's business associates
  - Vendor's third-party providers

Note: Non-profit organizations that have such identifiable information must comply with new regulations.

9

FTC Regulation Definitions: Health Information and Breaches Covered

- Elements for covered health information:
  1. Individual health information,
  2. Provided by or on behalf of the individual, and
  3. Identifies the individual or can be used to identify the individual.

- Elements triggering breach notification:
  1. Unauthorized acquisition,
  2. Unsecured information, and
  3. Identifies or could identify an individual

Title 16 of the Code of Federal Regulations Part 318.2

10

FTC Notification Regulations: Timing and Method

- Timing:
  - Notification must be made without unreasonable delay and in no case later than 60 days following discovery.
- Method:
  - Written notice by first-class mail unless individual intentionally opts to receive email notification
  - If more than 10 individuals cannot be contacted then:
    - Notice posted on website for 90 days, or
    - Notice in print or broadcast media where affected individuals reside

Title 16 of the Code of Federal Regulations Part 318.4 and 318.5

11

FTC Regulations: Content of Notice

- Notice shall describe:

1. What happened
2. Types of information breached
3. Steps individuals should take to protect themselves
4. Actions taken to investigate, mitigate harm, and protect against further breaches; and
5. Contact procedures to learn additional information

Title 16 of the Code of Federal Regulations Part 318.6

12

Not All Individually Identifiable Health Information is Covered

- Some government collections of individually identifiable health information are outside of new regulations
  - Information must be ”provided by or on behalf of the individual”
- Example of governmental database not covered:
  - Prescription Monitoring Program
    - Virginia’s Department of Health Professions

13

Joint JCHC and JCOTS Subcommittee Conclusions

Joint Subcommittee

Delegate Nixon	Senator Barker
Delegate O’Bannon	Senator Wampler

Joint JCHC and JCOTS Subcommittee Conclusions

- No action is needed pursuant to SB 1229
  - Objectives of SB 1229 have been satisfied by HITECH Act
- However, it would be useful for JCHC and JCOTS staff to review state and local government collections of individually identifiable health information that do not require breach notification
  - If appropriate, draft legislation to address this issue for 2010 Session

15

Policy Options

Policy Options

Option 1: Take no action.

Option 2: JCHC continue the study and include a report in the 2010 Workplan, if the current JCOTS and JCHC review is not completed in time for 2010 Session.

- Review focus: electronic individually identifiable health information records held by state and local government entities that do have legal requirements to notify individuals in the event of a breach.

17

Public Comment

- Written public comments on the proposed options may be submitted to JCHC by close of business on November 4, 2009.
- Comments may be submitted via:
  - E-mail: sreid@jchc.virginia.gov
  - Fax: 804-786-5538
  - Mail: Joint Commission on Health Care
P.O. Box 1322
Richmond, Virginia 23218
- Comments will be summarized and presented to JCHC during its November 12th meeting.

18

Additional Slides

Detailed Analysis: Federal Trade Commission Regulations on Health Information Breach Notification

FTC Regulations for Health Information Breaches for Non-HIPAA Covered Entities

1) Type of Entities Covered
2) Health Information Covered
3) Definition of a Breach
4) When Breaches Are Discovered
5) Timing for Notification
6) Notice Method to Individuals
7) Notice to Media and FTC
8) Content of Notice
9) Miscellaneous Provisions: Enforcement and Effective Date

20

1. Types of Entities Covered by FTC Regulations

1. ***Vendors of personal health records***
   a. Non-HIPAA covered entity that offers or maintains a personal health record.

2. ***PHR related entity - Non-HIPAA covered entity that***
   a. Offers products or services through the Web site of a vendor of personal health records
   b. Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records
   c. Accesses information in a personal health record or sends information

3. ***Third party service provider that***
   a. Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and
   b. Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.

Note: FTC regulations explicitly exclude HIPAA covered entities and HIPAA covered business associates.

Includes organizations outside of typical FTC purview, for example non-profits

Title 16 of the Code of Federal Regulations Part 318.2

21

2. Health Information Covered by FTC Regulations

PHR identifiable health information means:

''***individually identifiable health information***,'' as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information:

(1) That is provided by or on behalf of the individual; and

(2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Note: Health Information definition extends to even search-engine queries if search-engine on PHR website

Title 16 of the Code of Federal Regulations Part 318.2

22

3. What is a Breach?

- **Breach of security -** Acquisition of ***unsecured PHR identifiable health information*** of an individual in a personal health record without the authorization of the individual.
- Unauthorized acquisition will be ***presumed*** to include unauthorized access to unsecured PHR identifiable health information unless … reliable evidence shows … there has not been, or could not reasonably have been, ***unauthorized acquisition*** of such information.

Breach of PHR health information requires 3 main components:

1. ***Unauthorized acquisition***
2. ***Unsecured information***
3. ***Identifies or could identify an individual***

Title 16 of the Code of Federal Regulations Part 318.2

23

4. When Breaches Are Discovered

- A breach of security ***shall be treated as discovered*** as of the first day on which such breach is known or reasonably should have been known to the:
  - Vendor of personal health records,
  - PHR related entity, or
  - Third party service provider.
- Knowledge of breach is deemed if such breach ***is known, or reasonably should have been known***, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

Note: Time begins when breach should have been or is discovered

Title 16 of the Code of Federal Regulations Part 318.3

24

5. Timing for Notification

- Notification must be made without unreasonable delay and in no case later than 60 days following discovery.
  - 60 days outer limit for notice
  - Unreasonable delay can be found
- Burden of proof - entities have burden to show that appropriate and timely notifications were made
- Law enforcement exception for impeding criminal investigation or cause damage to national security

Title 16 of the Code of Federal Regulations Part 318.4

25

6. Notice Method to Individuals

- Written notice, by first-class mail to the individual at the last known address
  - May instead use email if "the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise this choice"
- If 10 or more individuals contact information is out of date, substitute notice shall be given by
  - Conspicuous posting for 90 days on the home page of the website, or
  - Major print or broadcast media in areas where individuals affected by breach are likely to reside
- In urgent situations when there is possible imminent misuse of unsecured PHR identifiable information, in addition to normal notifications, contact may be made by telephone and other means

Note: To opt out of mail notice individual has to intentionally chose email as preference

Title 16 of the Code of Federal Regulations Part 318.5

26

7. Notice to Media and FTC

- State and local media to be notified if breach involves more than 500 records
  - Includes if reasonable belief of breach
- FTC notification
  - All breaches of less than 500 records must be logged and reported annually
  - Breaches for 500 records or more require
    - Notice to FTC as soon as possible
    - 10 days is the maximum time to notify

Note : Breaches of secured data does not require notification

Title 16 of the Code of Federal Regulations Part 318.5

27

8. Content of Notice

Notice shall include in plain language:

A. Description of what happened
   - Includes: date of the breach and date of the discovery of the breach

B. Description of the types of unsecured PHR identifiable health information that were involved in the breach
   - For example: full name, social security number, date of birth, home address, account number, or disability code

C. Steps individuals should take to protect themselves

D. Description of actions taken to investigate, mitigate harm, and protect against any further breaches; and

E. Contact procedures
   - Includes: a toll-free telephone number, an email address, website, or postal address.

Title 16 of the Code of Federal Regulations Part 318.6

28

9. Miscellaneous Provisions: Enforcement and Effective Date

- Enforcement: Violation of FTC regulations are treated as "unfair or deceptive practice"
- Effective date: Late September 2009

Title 16 of the Code of Federal Regulations Part 318.7 and 318.8

29

Additional Health Information Regulations Pursuant to the HITECH Act

- Extending security rule applied to HIPAA Business Associates
  - Will define uses and disclosures of protected health information for business associates of HIPAA-covered entities
  - Will be similar to protections for HIPAA-covered entities
- Prohibited sale of electronic health information and allowed exceptions
  - Generally prohibits exchanging health information for remuneration without the individual's authorization

30