

Who needs caffeine when you have the stimulus bill

How the Recent Stimulus Plan Impacts Health Care Providers: What Every Compliance Officer Needs to Know

Session Facilitators

Frank Sheeder

Angelique Dorsey

Marti Arvin, JD, CHC, CCEP, CIPP/G, CPC
Privacy Officer
University of Louisville

American Recovery and Reinvestment Act – Part II

- Changes for Business Associates
- Breach Notification Provisions
- Enforcement Changes
- Restrictions on the sale of PHI from an EHR
- Other issues

Changes for Business Associates
– Part II

- Application of the Security Rule to Bas
 - Security Rule -
<http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf>
- Application of Privacy Rule to Bas
 - Privacy Rule -
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>

Business Associates & the Security Rule – Part II

- Administrative, physical and technical safeguard components –
 - “Required” vs. “Addressable”
- What constitutes “Addressable”

Business Associates & the Security Rule – Part II

- BAs must also have policies and procedures in place that address the administrative, physical and technical safeguards
 - The good news – Core of these policies exist
 - The “to do” is to get these plugged into your organization
 - Education Plan

Business Associates and the Privacy Rule – Part II

- The bill also applies the knowledge requirement of 45 CFR 164.504(e)(1)(ii)
- Pattern or Practice of breach
 - Discussion Point with CE - what is a “pattern or practice”
 - Revision of BAA with CE?

Breach notification provisions – Part II

- Provisions for covered entities
- Provisions for PHR vendors

Breach notification requirement for Covered Entities

- A breach is
 - Unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the privacy, security or integrity of the PHI.
- Breach does not include
 - Unintentional acquisition, access, use or disclosure of PHI to an employee or BA if done in good faith, in the normal course of employment or contract so long as it is not further acquired, accessed, used or disclosed by the employee or agent

Definition of Unsecure PHI

- Unsecure PHI is defined as
 - PHI not secured through technology or a method specified by the Secretary through guidance
 - If no guidance is provided by the Secretary by the deadline (60 days after enactment of the bill), then unsecure PHI shall mean PHI that is not secured by a technology standard that renders it unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standards development organization accredited by American National Standards Institute

10

Guidance from the Secretary

- Secretary issued guidance on 4/17/09
- Encryption is method for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals
 - Will look at method of encryption and whether the decryption key has been compromised
- The Secretary has asked for comment on whether PHI in a LDS should be deemed to fit the definition
- Paper PHI must be destroyed through shredding or another means to render it unreadable

11

American National Standards Institute Accreditation

- Example security related organizations accredited by ANSI include:
 - National Institute of Standards and Technology (NIST) Computer Security Division
<http://csrc.nist.gov/>
 - Information Technology Association of America
<http://www.ita.org/policy/infosec/>
 - Security Industry Association
<http://siaonline.org/default.aspx>

12

**American National Standards
Institute Accreditation – Part II**

- NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems
 - Appendix F - Assessment Procedures pages 77-359
 - Examples: Account Management, Remote Access, Security Awareness & Training, Audit Monitoring, Analysis and Reporting, Contingency Plan, Back-up, Incident Reporting, Risk Assessment...

**Breach notification requirement for
Covered Entities – Part II**

- A covered entity or BA is on notice of a breach on the first day anyone in the organization knows of the breach or reasonably should have known of the breach
- The covered entity or BA must notify the individual without unreasonable delay but no later than 60 days after breach is discovered.

**Breach notification requirement for
Covered Entities – Part II**

- Breach! - Now what do we do?
 - Policy/procedure
 - Process
 - Timeline
 - Delay documentation
 - Education / training of workforce - BA?
 - First Class mail, or
 - Other methodology if no known address
 - Documentation of efforts

Breach notification requirement for Covered Entities – Part II

- Policy/procedure - continued -
 - 10 person rule – if you don't have good information for at least 10 people – must list on home page/website or major print or broadcast media
 - Toll free number for individuals to call to inquire about impact

Breach notification requirement for Covered Entities – Part II

- Policy/procedure - continued -
 - Imminent danger – may notify by telephone
 - Less than 500- keep a log and submit to HHS Secretary annually
 - 500 person rule – The CE must:
 - Notify prominent media outlets in the state or jurisdiction where the individual resides
 - Must notify HHS Secretary
 - Immediate notice is required

Covered Entity - Content of the notification – Part II

- Brief description of
 - What happened
 - Unsecure PHI involved in breach
 - Steps the individual should take to protect themselves
 - The covered entity's investigation, mitigation of losses and corrective action plan
- Contact procedures for individuals to ask questions

Breach notification requirement for Covered Entities – Part II

- Deadlines:
 - Secretary has 180 days - August 17, 2009

 - 30 days after publication of the interim final regulations - September 16, 2009

Personal Health Records Vendors (PHR) – Part II

- Definition of PHR by the Office of the National Coordinator
- A PHR is
 - An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

Personal Health Records Vendors (PHR) – Part II

- PHR impact:
 - Breach Notification
 - FTC Notification
 - Third party service providers
 - Documentation of notification of breach

Breach Notification Requirements for PHR Vendors

□ Definitions:

- **Breach:** the acquisition of unsecure PHR individually identifiable health information of an individual without the person's authorization
- **Unsecure PHR:** identifiable health information is any information not secured through technology or methodology specified by the Secretary through guidance

22

Breach Notification Requirements for PHR Vendors – Part II

□ Policy/Procedure development:

- Required to notify individuals if there is a breach of their unsecure individually identifiable health information
- They must also notify the FTC. The FTC will notify the HHS Secretary
- Third party service providers of PHR vendors must notify the PHR vendor if they have a breach

23

Breach Notification Requirements for PHR Vendors – Part II

□ Documentation of breach:

- Brief documentation of what happened
- Identification of unsecured PHI involved in breach
- Steps the individual should take to protect themselves
- Investigation, mitigation of loss and Corrective Action Plan
- Inquiry process for affected individuals

24

**Breach Notification Requirements
for PHR Vendors – Part II**

- Documentation of breach (continued) :
 - More than 10:
 - Home web page
 - Major media outlet
 - Length of post
 - Toll free number

 - Imminent danger – notify immediately by phone

**Breach Notification Requirements
for PHR Vendors – Part II**

- Documentation of breach (continued) :
 - More than 500:
 - Notify major media outlet
 - Notify Secretary

 - Less than 500:
 - Keep log of breaches
 - Annual submission to HHS Secretary

**Breach Notification Requirements
for PHR Vendors – Part II**

- Deadlines: (same as CE)
 - Secretary has 180 days - August 17, 2009
 - 30 days after publication of the interim final regulations - September 16, 2009
- If a statute addressing breach notifications for all non-covered entities is enacted then this provision will sunset.

Enforcement Changes

- Changes to the CMP provisions of the HIPAA statute
- Enforcement allowed by State Attorneys General

28

Changes to the CMPs

- The new penalty ranges are
 - \$100 up to cap of \$25,000 for violations of each identical requirement or prohibition
 - \$1,000 up to cap of \$100,000 for violations of each identical requirement or prohibition
 - \$10,000 up to a cap of \$250,000 for violations of each identical requirement or prohibition
 - \$50,000 up to a cap of \$1,500,000 for violations of each identical requirement or prohibition

29

Enforcement and Changes to CMP – Part II

- Organizationally, what does this change?
 - Look back: How many incidents may have constituted a “breach”?
 - Reserves for litigation?
 - State Attorney General response?
 - Media Response?

30

State Attorney General can now bring a HIPAA action

- The ARRA provides for State Attorneys General to bring civil actions under HIPAA
- They are currently limited to pursuing \$100 per violation of an individual requirement or prohibition up to \$25,000 cap.
- It also allows for the Attorney General to seek attorney fees
- This provision is effective immediately

What determines which penalty will be imposed?

- If the violation is one that the covered entity did not know about and with the exercise of reasonable diligence would not have known about the Secretary has the discretion to impose the \$100 penalty up to the \$50,000 penalty

What determines which penalty will be imposed?

- If the violation is determined to be a reasonable cause and not willful neglect then the penalty range starts at \$1,000 and can go up to \$50,000 per violation
- If the violation is due to willful neglect and the covered entity corrects it within 30 days of discovery the penalty range starts at \$10,000 and can go up to \$50,000 per violation

What determines which penalty will be imposed?

- If the violation is due to willful neglect and the covered entity does not correct it within 30 days of discovery the penalty range starts at \$50,000 per violation
- A violation is deemed to be discovered when the covered entity knew or by exercise of reasonable diligence should have known that the failure to comply occurred.

Enforcement and Changes to CMP – Part II

- “Willful Neglect” - Why is this important?
 - Definition: (Marti?)
 - Remedy for Willful Neglect
 - Policy/procedures
 - Training
 - Other? (Marti??)
 - “Known & Should have known”
 - Why is that important?

Other issues for CEs – Part II

- Access to electronic records in EHR
- Request for restrictions
- Minimum necessary
- Accounting for disclosures
- Health care operations
- Sale of PHI from an EHR
- Marketing

CE – Electronic Access to Records
– Part II

- Patients currently have right to “Access” & a copy of their records
- New provisions will allow patients an electronic copy of their E-PHI if CE uses an EHR.
 - May designate person or entity to receive data
- IT / HIM issue: how to produce?

37

CE - Request for restrictions -
Part II

- If an individual requests a restriction under 164.522(a)(1)(i)(A), then the covered entity must comply with the request if
 - The disclosure is
 - Not otherwise required by law
 - To a health plan for payment or health care operations
 - AND
 - The PHI pertains solely to a health item for which the provider has been paid out of pocket in full

38

CE – Requests for Restrictions –
Part II

- Needed changes to Request for Restriction policy:
 - Health Plan related
 - Paid out of pocket
 - Paid in full
 - How do we capture electronically during claims submission?
 - How are we affected when Health Plan submits authorization from individual?

39

CE – Requests for Restrictions – Part II

- Needed changes to Request for Restriction policy: (continued)
 - Need IT at the table to “capture” those restrictions
 - Medical Records – must be aware of the restriction

CE - Minimum necessary – Part II

- Recap:
 - To the extent possible, disclosures should be in a LDS.
 - If a LDS is not feasible, minimum necessary should be applied.
 - Secretary to issue guidance on what constitutes minimum necessary within 18 months
 - The same exceptions to minimum necessary under HIPAA still apply

CE - Minimum necessary – Part II

- Exceptions (no changes):
 - health care providers for treatment purposes;
 - to the individual who is the subject of the information, or in response to an authorization requested by the individual;
 - to the Secretary of HHS when required for reviews or other enforcement purposes;
 - to meet the requirements of HIPAA or standard transactions; or
 - to comply with the requirements of other laws.

CE - Minimum necessary – Part II

- Guidance within 18 months -August 2010
- Policy revision:
 - “Payment” analysis of LDS usage
 - Patient Accounts
 - IT
 - “Operations” analysis of LDS usage
 - Compliance
 - Business Planning
 - Education
 - Consulting

43

CE - Accounting for disclosures – Part II

- If a disclosure from an electronic health record is made for treatment, payment or healthcare operations, an accounting is required.
- Accounting only goes back three years

44

EHR

- Definition give by Office the National Coordinator
- An EHR is
 - An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.

45

CE - Accounting for disclosures –
Part II

- Inventory of systems:
 - EHR
 - Lab systems
 - Others?
- What will this show?
 - Notice of Privacy Practices “How we may use your information”
- BA-Disclosures:
 - Disclosures by BA, how to coordinate
 - Discussion with BA on how this happens – contact information, etc

Accounting for disclosures – Part II

- Effective date
 - Current users (EHR was acquired on or before 1/1/09) of EHRs - 1/1/2014
 - New users (EHR acquired after 1/1/09) the later of 1/1/2011 or the date it acquires the EHR
- The Secretary can extend the effective date but there are limitations
 - No later than 1/1/16 for current users of EHRs
 - No later than 1/1/13 for new users of EHRs

Health Care Operations – Part II

- Secretary has 18 months to promulgate regulations that remove from the definition of HCO any activity that can be done with de-identified data or that would require an authorization.
- Begin to inventory your HCOs:
 - Legal, business planning, customer services, accreditation, evaluations of practitioners, etc.

Sale of PHI – Part II

- A covered entity cannot directly or indirectly receive remuneration in exchange for PHI without first:
 - obtaining an authorization that clarifies whether the party receiving the information can further exchange it for remuneration.
- The following are excluded from the requirement to obtain an authorization for the sale of PHI.
 - Research
 - If the payment for PHI is an amount reflects the cost for the preparation and transmittal of the data
 - Public health activities
 - Treatment of the individual

49

Sale of PHI – Part II

- Exceptions to the requirement for an authorization (cont.)
 - Payment is related to the sale, transfer, merger or consolidation of all or part of the CE
 - Payments to BAs for BA services
 - Payment is for providing the individual with a copy of their record
 - Other purposes defined by the Secretary

50

Sale of PHI – Part II

- Effective date – the Secretary has 18 months to promulgate regulations –August 2010
- This provision will be effective 6 months after the final regulations are implemented
- Need policy on Sale of PHI
 - Identification of the above items
 - Prohibition on Sale of PHI
 - Exclusions/Exceptions

51

Changes to Marketing – Part II

- Activities that were previously excluded from the definition of marketing are no longer considered health care operation if the covered entity gets paid for the activity.

52

Changes for Marketing – Part II

- Exceptions
 - If the communication if
 - Only for a drug or biological the individual is currently prescribed
 - The amount that the covered entity is paid for making the communication is a reasonable amount (reasonable amount will be defined by the Secretary in regulations AND
 - An authorization has been obtained from the patient OR


53

Changes to Marketing – Part II

- If the communication is made by the business associate on behalf of the covered entity and is pursuant to a contract an authorization is not required.
- Policy revision:
 - Paid activities
 - Exceptions
 - BA

54

QUESTIONS



55

Marti Arvin
Phone: (502) 852-3803
Email: marti.arvin@louisville.edu

56
