

HITECH Act of the ARRA and Implications on HIPAA

CMHPSM

Mental Health Provider Meeting

Friday, January 29, 2010

Origins

- Stimulus Package and American Reinvestment and Recovery Act (ARRA) gives in more incentives for electronic health information
- New kinds of entities holding health information
- Lack of controls and oversight by HIPAA protections
- Lack of HIPAA requirements on notifying people of breaches

Resulted in:

- Health Information Technology for Economic and Clinical Health (HITECH) Act

HITECH Act

- Title XIII of the ARRA of 2009, signed February 17, 2009
- New Definitions
- New Breach Notification requirements
- New expectations of Protections (EHR)
- New kinds of Covered Entities
- New/additional Enforcements, Audits, and Penalties
- Effective Dates

New Definitions in HITECH

- “**Breach**” the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.
- Poses a significant risk of financial, reputational, or other harm to person
- Exceptions are: unintentional or inadvertent by an employee /staff if in good faith, in scope of job, and without further acquisition, access, use, or disclosure by any person

New Definitions

- **Electronic Health Record**

An electronic record of health-related information created, gathered, managed, and consulted by clinicians and staff

Qualified Electronic Health Record includes demographic and clinical health information, i.e. medical history and problem lists. Has the capacity to provide clinical decision support, support physician order entry

New Definitions

- **Personal Health Record**

an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

HITECH Effects on HIPAA

- Business Associates
 - now covered under HIPAA (same regs. as Covered Entities)
 - Security and privacy Rules now apply to BAs
 - Information can only be used per contract language
 - Penalties now apply to Bas
 - BAs accountable for BAAs
 - Held to Health Information Exchanges Health Information Exchanges

Breach Notification

- Effective 2/22/2010, for breaches of unsecured information occurring on or after 9/23/09
- Encryption methods must meet HIPAA **and** HITECH regulations (HITECH more stringent)
- Unsecured information defined(13402(h)(2))
- Need to follow NIST (National Institute Standards of Technology) guidelines with securing electronic health information
- FIPS 140-2 Publication of NIST

<http://csrc.nist.gov/groups/STM/index.html>

Breach Notification-Individual

- Individuals must be notified when their unsecured protected health information has been, or is reasonably believed by the CE/BA to have been, accessed, acquired, or disclosed as a result of such breach.
- Breach is treated as discovered by a CE/BA as of 1st day on which such breach is known to such entity or associate, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

Breach Notification-Individual

- Notification must happen without delay, no later than 60 days
- Specific requirements for Content of Notice
 - plain language
 - what happened, date and discovery of breach (if known)
 - Information breached
 - Steps to take for protection
 - What CE/BA is doing about it (investigation, lessening impact, protecting from future breaches)

Breach Notification-Individual

- Contact information (toll free #, email, address, website)
- Method of Notice
 - mail, email, multiple (phone if urgent)
 - Next of kin if deceased
 - Post on website/major media for 90 days if no contact for over 10 days (with toll free #)
- Notification to Media –if more than 500 affected
 - Within 60 days
 - Same info. as individual notice

Breach Notification - Others

- Notification to Secretary of HHS
 - If over 500 affected
 - Secretary of HHS will post on website
 - Annual report of ALL breaches to Secretary of HHS
- BAs must notify CEs
- Some allowable notification delays for Law Enforcement
- Compliance w/Privacy Rule
- Burden of proof on CE/BA to show notice given and determination of not a breach

Breach Reporting

Requirements to WCHO as CE

- Any breach that would be a potential Recipient Rights issue **MUST** be reported to ORR in required ORR reporting timeframes
- Data on breaches for all providers/CEs/BAs needs to be kept
- Data needs to be reported quarterly to WCHO as CE
- Data needs to be reported quarterly to HHS (1st report due 3/1/10)

Accounting of Disclosures

- New Rules for **EHRs** – need to provide on request
- Can list by CE and BA, or just list CE disclosures and identify the BAs to ask for accounting from
- BAs can be directly asked for an accounting
- Exceptions Privacy Rule has exception for Treatment, Payment, & Healthcare Operations (TPO) – ***will no longer apply when EHR is used***
 - Accounting for EHR goes back 3 years
 - If using EHR before 1/1/09, effective 1/1/2014
 - If began using EHR after 1/1/09, effective 1/1/2011

Restrictions of Disclosures

- Person can request no disclosure to insurance of paid out of pocket (effective 2/17/10)
- Must provide only limited data set or minimum necessary (guidance 8/10)
- Disclosers will need to determine minimum necessary (will need potentially need to defend); used to be requester's determination.
- No sale of PHI without authorization specifically allowing compensation (marketing)

Enforcement

- Wrongful disclosures
 - Now applies to CEs, Bas and individuals (2/17/10)
- Audits of CEs and Bas by HHS will begin 2/17/10
- Willful neglect violations
 - Must be investigated; mandatory penalties
- Four categories of violations that reflect increasing levels of culpability;

Enforcement

- Four corresponding tiers of penalty amounts that significantly increase the minimum amount for each violation; and
- A maximum penalty amount of \$1.5 million for all violations of an identical provision.
- Strikes previous imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and

Enforcement

- Providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

Timeframes

Immediately in Effect

Penalties

Enforcement of HIPAA by State AG

Logging of Breaches back to 9/23/09

February 17, 2010

Revised BA Agreements Due

HIPAA applies to BAs

Restriction of Disclosures

Wrongful Disclosures Penalties

HIPAA Audits by HHS

Timeframes

March 1, 2010

1st Breach log due to HHS

August 17, 2010

Regulations effective on: sales of PHI, willful neglect

Guidance on minimum necessary & psychotherapy notes due

January 1, 2011

Provide accounting of disclosures (includes TPO) if began using EHR after 1/1/09

January 1, 2014

Provide accounting of disclosures (includes TPO) if began using EHR before 1/1/09

Resources

HIPAA and HITECH Information

- <http://www.hhs.gov/ocr/privacy/index.html>
- <http://www.hipaasurvivalguide.com/>

Guidelines for breaches and secure PHI

- <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/federalregisterbreachrfi.pdf>

Guidelines for NIST standards on security

- <http://csrc.nist.gov/groups/STM/index.html>

Questions/Contact Information

**CJ Witherow, LMSW, CAAC
Chief Compliance Officer for CMHPSM**

555 Towner

Ypsilanti, MI 48197

Office: 734-544-6819

Fax: 734-544-6732

Work Cell: 734-660-0778

Email: witheroc@ewashtenaw.org