



New Challenges with HITECH: Changes in Privacy and Security Rules

Robert M. Tennant, MA
Senior Policy Advisor
Medical Group Management
Association
rtennant@mgma.com
202-293-3450



Objectives

- Identify the new requirements placed on your practice by the ARRA statute and related regulations;
- Understand the timeline for the government's implementation of these requirements; and
- Recognize the steps your practice will need to take to prepare for these changes and avoid government enforcement action.



Overview

- Individual's Right to Access to PHI
- Minimum Necessary
- Individually Requested Privacy Restrictions
- Extension of HIPAA to business associates (BAs)
- Federal breach notification and reporting rules applicable to covered entities (CEs)
- Accounting of disclosures
- Marketing
- No Sale of PHI
- New Enforcement Approaches and Penalties

Copyright 2010. Medical Group Management Association. All rights reserved.

3



HIPAA and HITECH

- Why HITECH Matters:
- 1996 HIPAA Administrative Simplification
 - Standards for administrative and financial transactions to promote efficiency and cost savings
 - HIPAA Privacy and Security embedded as applicable law to protect consumer interests
- 2009 HITECH Act of ARRA
 - Significant incentives for adoption and meaningful use of electronic health records
 - Standards for electronic records and data sharing in clinical setting, for quality reporting, and other population health purposes
 - Subpart D for privacy protections and security for patient identifiable information

Copyright 2010. Medical Group Management Association. All rights reserved.

4



HIPAA and HITECH-Why People Care

- Successful acceptance of EHRs and PHRs will require earning public's trust their PHI will be kept private and secure
- 70% of adults surveyed are worried that sensitive health information might leak because of weak security
- 62% of adults are concerned that existing federal health privacy rules of protecting patient information will be reduced in the name of efficiency
- 69% believe strong enough data security will not be installed in the NHIN



Copyright 2010. Medical Group Management Association. All rights reserved.

5



Current Environment

- Many providers lack basic security technologies and processes
- Security spending lags behind other regulated industries
- Providers moving to electronic health records (EHR) without considering security implications
- Hackers increasingly targeting healthcare and medical facilities



Copyright 2010. Medical Group Management Association. All rights reserved.

6



Where are Your Risks?

- Loss of financial data
- Permanent loss of confidential information
- Temporary loss of medical records
- Unauthorized access to confidential information
- Loss of physical assets (i.e., computers, PDAs)
- Damage to practice reputation, patient confidence
- Government enforcement

Copyright 2010. Medical Group Management Association. All rights reserved.



What are Your Threats?

- Current employees (most common)
- Former employees
- Patients / visitors
- Vendors
- Commercial rivals
- Hackers / criminals / terrorists

Copyright 2010. Medical Group Management Association. All rights reserved.



Typical Security “Events”

- Unauthorized access by employees
- Misuse of authorized access
- Physical disasters
- Server crashes
- Staff untrained on dealing with security issues
- Ineffective disposal of PHI (i.e., computer disks)



Copyright 2010. Medical Group Management Association. All rights reserved.

History of HIPAA Enforcement

- 48,000 complaints received by Department of Health & Human Services (HHS)
- Vast majority resolved through voluntary compliance or corrective action
- Two “Resolution Agreements”
- Handful of criminal prosecutions



Copyright 2010. Medical Group Management Association. All rights reserved.

10

Individual's Right to Access to PHI



- Existing law: Individual has a right to access/receive a copy of medical record (45 CFR 165.524)
- HITECH: If CE uses/maintains an EHR
 - Right to electronic copy of records
 - Right to direct CE to transmit electronic copy to another entity or person
 - Practice options include media such as CD-ROM, USB drives, Websites
 - An element of “meaningful use” for Medicare/Medicaid incentives
 - Effective: February 18, 2010

Copyright 2010. Medical Group Management Association. All rights reserved.

11



Minimum Necessary



- Preference for Limited Data Sets and de-identified information
- Disclosure should be of the limited data set or, if not practical, the “minimum necessary” information to accomplish the purpose of the disclosure
- Minimum necessary is determined by the disclosing party
- Exclusions for disclosures for treatment and law enforcement retained
- Effective: 2/18/10; Regulations required by 8/18/10

Copyright 2010. Medical Group Management Association. All rights reserved.

12



Individually Requested Privacy Restrictions



- Existing Law: Individual has right to request privacy restrictions but binding on CE only if CE agrees
- HITECH: No disclosure to health plans for self-pay services
- Effective: 2/18/10
- Particularly important for certain specialties/settings
- Key impact area-record keeping (i.e., plan requests for records)

Copyright 2010. Medical Group Management Association. All rights reserved.

13



Business Associates



- Existing Law: BAs have not been directly regulated by HIPAA
 - Instead Covered Entities were required to enter into BA contracts with their BAs.
 - Way to backdoor some of the HIPAA requirements
- HITECH: BAs directly regulated effective 2/18/10 (except as noted)

Copyright 2010. Medical Group Management Association. All rights reserved.

14



Business Associates



- HITECH clarification of BA status
 - HIEs
 - RHIOs
 - e-Prescribing Gateway
 - PHR vendors that provide PHRs to CEs

Copyright 2010. Medical Group Management Association. All rights reserved.

15



Business Associates



- HITECH: BAs are required to:
 - Directly comply with administrative, physical and technical safeguards and documentation requirements under the HIPAA security rule — as if they were CEs
 - Not use or disclose PHI in a manner that is not in compliance with the privacy portions of their BA contracts
 - Notify CEs if they discover a data breach (Effective 9/23/09)

Copyright 2010. Medical Group Management Association. All rights reserved.

16



Business Associates



- Other HITECH privacy and security requirements that apply to CEs will be applicable to BAs and shall be incorporated into BA agreement
- Implications for existing BA agreements:
 - Amendment of existing agreements probably not required
 - Notice to BAs of new obligations a better practice
 - Make reference to new obligations in new BA agreements

Copyright 2010. Medical Group Management Association. All rights reserved.

17



Business Associates



- BAs now obligated to comply with BA requirements with respect to BA's subcontractors (question: are BA's subcontractors BAs for purposes of HITECH?)
- BAs now subject to civil and criminal enforcement and penalties under HIPAA
 - Criminal enforcement has always been a possibility
 - Civil enforcement and audits are new

Copyright 2010. Medical Group Management Association. All rights reserved.

18



Expanded Accounting of Disclosures



- Existing law: No TPO in accounting
- HITECH: if CE uses/maintains an EHR
 - Right to accounting of disclosures including TPO through EHR
 - 3-year period (as opposed to 7 in existing law)
 - Fees = labor costs
- Affected by rulemaking (within 6 months)
- Compliance Dates: 1/11/11; existing EHRs (as of 1/1/09) have until 1/1/14
- Practices should raise this issue with current/prospective EHR vendors
- Element of “meaningful use” for Medicare/Medicaid incentives

Copyright 2010. Medical Group Management Association. All rights reserved.



Notification in Case of Breach – The Rule



- First federal mandatory breach notification requirement imposed on HIPAA CEs and BAs eff. 9/23/09
- The rule: Each CE that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured PHI must notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired or disclosed due to a breach (HITECH Section 13402(a), 42 USC §17932(a); 45 CFR Parts 160, 164 (pub. 8/24/09))
- Burden of proof compliance is on CE

Copyright 2010. Medical Group Management Association. All rights reserved.

20



Breach – What is it?

- “Breach” means unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the PHI (*i.e.*, poses a significant risk of financial, reputational or other harm to the individual)
- “Access” means the ability to read, write, modify or communicate data or otherwise use any system resource

Copyright 2010. Medical Group Management Association. All rights reserved.

21



Breach – What is it?

- “Breach” does not mean
 - By authorized persons:
 - Unintentional acquisition or use in good faith in the course and scope of employment to someone authorized to access PHI OR
 - Inadvertent disclosure by an authorized person to another authorized person within the same CE or BA
 - AND the information is not further acquired, accessed, used, disclosed
 - By CE or BA, if good faith belief that the disclosure was to an unauthorized person who would not be able to retain the PHI

Copyright 2010. Medical Group Management Association. All rights reserved.

22



Breach – “Unsecured PHI”

- Per guidance of HHS issued April 17, 2009: PHI is secure if it is rendered unusable, unreadable or indecipherable to unauthorized individuals by
 - Encrypted and process or key has not been breached: examples in National Institute of Standards and Technology (NIST) publication 800-111, Federal Information Processing Standards (FIPS) 140-2
 - Media is destroyed
 - Media is purged consistent with NIST publication 800-88

Copyright 2010. Medical Group Management Association. All rights reserved.

23



Breach – Limited Data Set + is Secure

- Per 8/24/09 Regulations: data consisting of the limited data set (45 CFR section 164.514(e)(2)), not including date of birth and zip code is not subject to breach notification because its disclosure does not compromise the security or privacy of PHI

Copyright 2010. Medical Group Management Association. All rights reserved.

24



"Significant Risk of Harm"

- Risk of Harm Assessment/Factors to Consider
 - Type and amount of information disclosed
 - Likelihood that the information is accessible and usable
 - Likelihood that breach will lead to harm to individual
 - Steps taken to mitigate harm to individual

Copyright 2010. Medical Group Management Association. All rights reserved.

25



Breach – Patient Notification

- "Without reasonable delay" – 60 days after discovery by a work force member or agent of the CE (or would have been discovered with reasonable diligence)
- Recordkeeping of notifications
- First class mail or email if requested (multiple mailings if required)
- Next of kin if subject is deceased
- Substitute if contact information out of date or insufficient (may be informal if less than 10 subjects)

Copyright 2010. Medical Group Management Association. All rights reserved.

26



Breach – Patient/Other Notification



- If imminent danger – telephone or other means in addition to required notice
- Plus, if more than 500 residents of a state or region are affected, CE must:
 - Promptly disclose to prominent media outlets after discovery at the same time notify Secretary of HHS
- Annual notice to Secretary if fewer than 500 subjects
- Notice can be delayed at request of law enforcement

Copyright 2010. Medical Group Management Association. All rights reserved.

27



Breach – Notification -- Contents



- What happened, date of discovery and date of breach
- Types of unsecured PHI involved (*e.g.*, whether full name, SS#, DOB, home address, account #, diagnosis, disability code)
- Steps affected individuals should take for protection
- Investigation, mitigation and protection measures by CE
- Contact information including toll-free number, e-mail address, website or postal address

Copyright 2010. Medical Group Management Association. All rights reserved.

28



Breach – Business Associates

- Business Associates (BAs) must provide CE with notice of breach, including
 - identification of each subject
 - any other available information that the CE is required to include in CE's notice



Copyright 2010. Medical Group Management Association. All rights reserved.

29



Avoiding Breach Notification: Encryption Safe Harbors

- Valid processes for encryption of stored PHI include those consistent with NIST Special Publication (“SP”) 800-111, *Guide to Storage Encryption Technologies for End User Devices*, including (but not limited to) full disk encryption, volume encryption, virtual disk encryption, and file/folder encryption
- Valid processes for encrypting PHI during transmission would be those complying with the requirements in Federal Information Processing Standard (“FIPS”) 140-2, including NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*, 800-77, *Guide to IPsec VPNs*, or 800-113, *guide to SSL VPNs*



Copyright 2010. Medical Group Management Association. All rights reserved.

30



Avoiding Breach Notification: Destruction



- To comply with the destruction guidance, the media on which the PHI is stored or recorded must be destroyed in the following ways:
 - Hard copy media (such as paper and film) must be shredded or destroyed in such a way that PHI cannot be read or otherwise reconstructed
 - Electronic media must be cleared, purged, or destroyed so that the PHI cannot be retrieved, consistent with the NIST SP800- 88, *Guidelines for Media Sanitization*



Copyright 2010. Medical Group Management Association. All rights reserved.

31

What Role Does HIPAA Play in Security Breaches?



- The HIPAA Privacy Rule requires covered entities to:
 - Mitigate – Must mitigate any harmful effects of unauthorized disclosure (police reports, notification)
 - Sanction – Must apply appropriate sanctions against employees who fail to comply with privacy and security policies and procedures
 - Account for Disclosures – Unauthorized disclosures of PHI must be accounted for on accounting log
- Other Compliance Efforts:
 - Training – Retrain employees
 - Policies and Procedures – Evaluate effectiveness of and modify, if appropriate, policies, procedures and safeguards
 - In the event of a breach, likely that CEs will receive a request from HHS-OCR and/or CMS asking for a description of the incident and details regarding the safeguards that were in place or have been put in place since the breach to protect the privacy and security of PHI



Copyright 2010. Medical Group Management Association. All rights reserved.

32

Breach - Implications for Policy Development



- Regulations are effective 9/23/09
- Important elements
 - Technology: measures to ensure all PHI is secure
 - Leadership and responsibility
 - Role of legal counsel for compliance, privilege protections
 - Reconciliation with state requirements
 - Training
 - Before
 - After
 - BA compliance
 - Amending BA agreements
 - Aligning processes and procedures
 - Complaint mechanism regarding policies and procedures, compliance

Copyright 2010. Medical Group Management Association. All rights reserved.

33



Breach – Policy Development



- Practices should develop:
 1. Processes for discovering breaches
 2. Procedures and forms for reporting
 3. Mechanisms for determining
 - if unsecured PHI involved
 - individuals affected
 - applicable notification requirements
 4. Processes for
 - determining appropriate mitigation
 - developing advice to affected individuals
 - creating and distributing notices
 - determining and creating other forms of communication
 - accounting for notification
 - reporting to Secretary of HHS

Copyright 2010. Medical Group Management Association. All rights reserved.

34



Practice Action Steps-Breach



- Create/refine your breach response plan:
 1. Identify your team
 - Internal
 - Line up potential external resources
 2. Develop breach notice form, policies, response flow chart
 - Don't forget state law
 3. Insurance options
 4. Practice drill(s)

Copyright 2010. Medical Group Management Association. All rights reserved.

35



Marketing



- Existing Law: exceptions to “marketing” (treatment, care coordination, part of plan of benefits, etc.)
- HITECH: Exceptions do not apply if CE receives direct or indirect payment for communication unless:
 - payment is for a communication regarding a drug currently prescribed for the recipient if the communication and such payment are “reasonable in amount”
 - the communication is made by the CE and the CE obtains a valid authorization in accordance with HIPAA section 164.508 from the recipient; or
 - the communication is made by a BA of a CE, on behalf of such CE, and such communication is consistent with the applicable BA agreement
- Effective: 2/18/10

Copyright 2010. Medical Group Management Association. All rights reserved.

36



No Sale of PHI



- Existing law: Except in the area of marketing, the HIPAA privacy rule does not prohibit a CE from being paid for PHI as long as the disclosure is otherwise permitted
- HITECH: Prohibits a CE or BA from directly or indirectly receiving remuneration in exchange for any PHI without a valid authorization from the individual that includes a specification of whether the protected health information may be sold by the entity receiving the PHI
- Effective: 2/18/10

Copyright 2010. Medical Group Management Association. All rights reserved.

37



No Sale of PHI



- Exceptions:
 - Public health activities
 - Research and the price reflects the costs of preparation and transmittal
 - Treatment of the individual, subject to any regulation
 - Sale, transfer, merger or consolidation

Copyright 2010. Medical Group Management Association. All rights reserved.

38



Additional Limitations: Marketing



- HITECH Act placed limitations on the marketing exception. If payment received for making the communications, the communication is marketing, unless:
 - The communication describes only a drug or biologic currently being prescribed for the individual and the amount of payment received for making the communication (if any) is reasonable in amount;
 - The communication is made by the covered entity and the covered entity has received a valid HIPAA authorization from the individual to whom it is making the communication; or
 - The communication is made by a BA and is consistent with the terms of its BA associate agreement with the practice

Additional Limitations: Fundraising



- HHS required to issue a rule that requires all written fundraising communications to provide the recipient with an opportunity to opt out of any future fundraising communications
- Different from the Privacy Rule, the HITECH Act now requires CEs to treat an individual's election to opt out of fundraising communications as a revocation of authorization

New Enforcement Approaches



- Civil penalties for unknowing, knowing and willfully neglectful violations of HIPAA
- Civil money penalties to be shared with enforcers and harmed individuals
- Clarifies/expands who is liable for criminal violations: apply to unauthorized individuals who obtain or disclose PHI maintained by a CE
- Effective: 2/17/09

Copyright 2010. Medical Group Management Association. All rights reserved.

41



New Penalties



- Tier A (if offender did not know, and by exercising reasonable diligence would not have known, that he or she violated the law): \$100 for each violation, up to \$25,000 for identical violations
- Tier B (if the violation was due to reasonable cause and not willful neglect): \$1,000 for each violation, up to \$100,000 for identical violations
- Tier C (if the violation was due to willful neglect but was corrected): \$10,000 for each violation, up to \$250,000 per year
- Tier D (if the violation was due to willful neglect and was not corrected): \$50,000, up to \$1,500,000 per year

Copyright 2010. Medical Group Management Association. All rights reserved.

42



State Attorneys General May Act Under HIPAA



- §13410(e), effective immediately (2/17/09)
- State AGs can bring Civil Action in Federal Court
- Can enjoin violations and obtain damages
- Damage awards can be up to \$25,000 per violation, per year
- Action by DHHS pre-empts State AG action

Copyright 2010. Medical Group Management Association. All rights reserved.

43



Proactive Audits



- §13411, effective February 17, 2010
- Secretary of DHHS will provide periodic audits of CEs and BAs for compliance with the HIPAA Privacy and Security Rules
- No longer complaint-based audits only
- Audit process in planning

Copyright 2010. Medical Group Management Association. All rights reserved.

44



HITECH Enforcement Context



- Review of key changes:
 - Business Associates liable for criminal and civil penalties
 - Compliance audits required
 - State Attorneys General expressly authorized to enforce
 - Enforcement funding and, by 2012, percentage of CMPs/settlement distributed to individuals
 - Explicit authority to seek criminal penalties for wrongful disclosure of protected health information (PHI)
- Net effect:
 - More aggressive enforcement
 - Higher penalties
 - More potential opportunities for enforcement

Copyright 2010. Medical Group Management Association. All rights reserved.

45



HITECH and Enforcement - Forthcoming Rulemakings and Other Provisions



- Forthcoming Enforcement Regulations:
 - Violations that are Criminally Punished
 - Noncompliance Due to Willful Neglect
- Distribution of Certain Civil Monetary Penalties
- Other Provisions:
 - State Attorneys General
 - Criminal Penalties for Individuals (Employees)
 - Audits

Copyright 2010. Medical Group Management Association. All rights reserved.

46



Penalties/Enforcement/Audits To-Do List...



- ✓ Don't be in denial – willful neglect will cost you
- ✓ Implement full Privacy and Security Rule compliance including risk assessment, policies, procedures, etc.
- ✓ Develop your breach notification policy and plans– you need this for state laws and start logging breaches now
- ✓ Be ready for February 2010: wrongful disclosures penalties in effect, HHS audits begin
- ✓ Be ready for August 2010: regulations on willful neglect due, in effect by February 2011

Copyright 2010. Medical Group Management Association. All rights reserved.

47



Guidance for Practices



- Identify systems that have covered data
- Secure your PHI – Encrypt or Destroy
- Evaluate existing privacy and security policies and procedures and assess whether current administrative, technical and physical safeguards are sufficient to protect the privacy and security of PHI.
- Work with your Chief Information Officer or IT/IS Managers to determine whether you currently encrypt or have the capabilities to encrypt PHI (the cost of encryption likely is less expensive than addressing a security breach)

Copyright 2010. Medical Group Management Association. All rights reserved.

48



Guidance for Practices



- Assign internal roles and responsibilities, and identify external vendors
- Review your medical record retention and destruction policies to confirm that data is being destroyed properly
- To reduce risk, do not retain medical records longer than necessary
- Consider incident response insurance policies

Copyright 2010. Medical Group Management Association. All rights reserved.

49



Steps to HIPAA Compliance



1. Begin with a thorough risk assessment
2. Review all current policies and procedures (gap analysis)
3. Identify all locations with PHI
4. Determine whether encryption is warranted, and to what extent
5. Create a cost-effective plan to mitigate top risks (i.e., physician laptops)

Copyright 2010. Medical Group Management Association. All rights reserved.

50



Steps to HIPAA Compliance



6. Ensure BA contracts are modified
7. Update policies and procedures
8. Train impacted staff
9. Take a cross-functional approach to compliance
10. This is a good opportunity to do a HIPAA house-cleaning!
11. "HIPAATIZE" your staff!!

Copyright 2010. Medical Group Management Association. All rights reserved.

51



Key Take-Aways



- ✓ Expect more enforcement and bigger penalties for HIPAA violations
- ✓ Have a well-thought out breach response plan before the breach occurs
- ✓ Managing a breach correctly after it occurs requires understanding its scope and extent
- ✓ Basic safeguards can help prevent a breach or, if it does occur, can minimize its impact
- ✓ Expect many more regulations!

Copyright 2010. Medical Group Management Association. All rights reserved.

52



Thank you!

Q&A



Resources

- The OCR website (guidance, FAQs, all regulations and announcements): <http://www.hhs.gov/ocr/privacy/>
- Breach Notification Interim Final Rule (74 FR 42740): <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>
- Enforcement Interim Final Rule (74 FR 56123): <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitech enforcementifr.html>
- National Institute of Standards and Technology: www.nist.gov

