AFTER THE OMNIBUS RULE

Agenda

- Omnibus Rule
- Business Associates (BAs) Agreement
- Breach Notification Change
- Breach Reporting Requirements (Federal and State)
- Notification to Care1st Health Plan
- Member Breach Notification Timeframes

OMNIBUS HITECH FINAL RULE:

- The Health Information Technology for Economic and Clinical Health Act (HITECH) Final Rule (Omnibus) released on January 17, 2013 and published January 25, 2013 in the Federal Register http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

- The HIPAA Omnibus Rule implements the HITECH Act provision making Business Associates (BAs) and BAs' downstream subcontractors, directly accountable for compliance with the Health Insurance Portability and Accountability Act's (HIPAA) Security and Privacy Rule requirements.

- Compliance Deadline for Covered Entities and Business Associates was September 23, 2013.

HITECH FOCUS AREAS FOR BUSINESS ASSOCIATES:

- Business Associates' HIPAA/HITECH Obligations:
  - Direct HIPAA Compliance with Security Rule (i.e., written policies & Security Assessment)
  - Direct HIPAA Compliance with applicable sections of Privacy Rule
  - HIPAA BA agreements and sub-vendor BA agreements
- Security Breach Notifications
  - "Presumption" Breach
  - Specific Exceptions, or documented breach risk assessment
  - Who must BAs notify?
  - When must BA notify?
- Business Associate Agreements

HIPAA Definition: "Business Associate"

- 45 C.F.R. §160.103: A Business Associate (BA) is a person / entity who / that:

  (i) ***On behalf of such covered entity (CE)*** or of an organized health care arrangement (OCHA) in which the CE participates, ***but other than in the capacity of a member of the workforce*** of such CE or arrangement, *performs, or assists* in the performance of:

  A. a ***function or activity*** involving the ***use or disclosure of PHI***, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or

  B. Any other function or activity regulated by subchapter; OR

HIPAA Definition: "Business Associate" – continued:

- 45 C.F.R. §160.103: A Business Associate (BA) is a person / entity who / that:

  (ii) Provides, *other than in the capacity of a member of the workforce* of such CE, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501), management, administrative, accreditation, or financial services to or for such CE, or to for an OHCA in which the CE participates, where the provision of the service involves the disclosure of PHI from such CE or arrangement.

HITECH FINAL RULE: Expanded Definition of a "Business Associate"

- Now specifically includes:
  - E-prescribing gateways
  - Vendors providing service on behalf of a covered entity (CE)
  - Health information organizations

HITECH FINAL RULE: Expanded Definition of a "Business Associate" continuation…

- Any person or entity that transmits PHI or requires access to PHI on a ***routine*** basis:
  - **Conduits** for data transmission are NOT BAs (e.g., retains PHI for only that period of time necessary to support transmission process)

BA's SUB-CONTRACTORS TOO!

- Any person or entity that "creates, receives, maintains or transmits" PHI on behalf of a HIPAA Business Associate (45 CFR 160.103(3)(iii);
- This applies even if sub and BA don't enter in a Business Associate Agreement (BAA);
- The HIPAA / BAA obligations attach to **downstream** subcontractors too!
- The Office of Civil Rights (OCR) can directly enforce requirements against subcontractors.

CAN BAs AND SUB-BAs AVOID HIPAA?

- **The absence of a BA Agreement does <u>NOT</u> mean that a BA can avoid HIPAA compliance.**
  - A BA is determined by HIPAA's definitions and the activities of the BA (or sub), and direct compliance and enforcement by OCR cannot be avoided by simply not having in place a HIPAA-compliant BA Agreement in place between the CE and the BA, or the BA and its Sub-Contractor.

CAN BAs AND SUB-BAs AVOID HIPAA? Continuation…

- **Just because you are not a BA, does NOT mean HIPAA is nor relevant.**
  - If you do not need access to a CE's PHI to perform a "service or function" on "behalf of" such Covered Entity, then not only are you likely not a BA, **but you might also not have the authority to be accessing or using such PHI.**

BREACH NOTIFICATION

SECURITY BREACH NOTIFICATION

- HITECH INTERIM BREACH RULE:
  - Defined a Breach to mean generally: " the acquisition, access, use, or disclosure of protected health information (PHI)in a manner not permitted [by the Privacy Rule] **which compromises** the security or privacy of the phi."
  - If further elaborated that "compromises" the security or privacy of the PHI meant **poses a significant risk** of financial, reputational, or other harm to the individual.
    - Note: HHS originally included "harm" test in order to align the rule with many State breach notification laws as well as existing obligations on Federal Agencies that have a similar "risk of harm" standard for triggering breach notification.

SECURITY BREACH NOTIFICATION

- HITECH FINAL RULE:
  - Removes the "significant risk of harm" test, and replaces it with a *presumption* that any impermissible use or disclosure of PHI is **presumed to be a breach** unless the CE or BA demonstrates that there is a **low probability** that the PHI has been compromised.
  - CE or BA has the **burden of proof** to demonstrate that there is a low probability that the PHI Is compromised. The CE or BA must also **maintain written documentation** sufficient to demonstrate why it concluded that there is a low probability that the PHI was compromised and did not issue notices (e.g., a HIPAA Risk Assessment tool).

BREACH UNDER FEDERAL LAW

Element	HITECH	OMNIBUS
Who is Covered?	Covered Entities (CEs) and Business Associates	Same
What Information?	Protected Health Information	Same
What *Medium*?	Electronic, Paper, and Oral	Same

WHEN IS SECURITY INCIDENT A BREACH?

Element	HITECH	OMNIBUS
"Breach" defined	• Unauthorized acquisition, access, use, disclosure, i.e., violation of Privacy Rule •Unsecured PHI	• Unauthorized acquisition, access, use, disclosure i.e., violation of Privacy Rule •Unsecured PHI •Presumption of Breach
Unauthorized Access	A use or disclosure in violation of the Privacy Rule	Same
"Secured" vs. Unsecured	Unusable, unreadable, indecipherable by: - Encryption, Destruction, and Per National Institute of Standards and Technology (NIST) Standards	Same
Compromises	~~Significant "Risk of Harm"~~	Low Probability PHI Compromised

SAFE HARBORS: EXCEPTIONS & KNOWLEDGE

Element	HITECH	OMNIBUS
Unintentional	• Acquisition, access or use •By ~~employee or agent~~ of CE or BA •Good Faith •Within scope of authority •Nor further violation of Privacy Rule	• Acquisition, access or use •By workforce member or person acting under the authority •Good faith •Within scope of authority •No further violation of Privacy Rule
Inadvertent	• Disclosures •By E~~mployee or Agent~~ of CE or BA •To ~~Employee or Agent~~ at same CE/BA •No further violation of Privacy Rule	•Disclosures •By workforce member or person acting under the authority of CE or BA •To workforce member at the same CE/BA •No further violation of Privacy Rule

SAFE HARBORS: EXCEPTIONS & KNOWLEDGE

Element	HITECH	OMNIBUS
Retention Not Possible	•Disclosure to unauthorized person •Good faith belief that unauthorized recipient would not be able to retain the PHI	Same
Knowledge	• Actual knowledge (including imputed knowledge of employees and agents) •"Should've known" with reasonable diligence	Same

"LOW PROBABILITY" PHI COMPROMISED

Four (4) Factors (Risk) Assessment

Nature and Extent of PHI involved, including the types of identifiers and the likelihood of re-identification.	Consider the type of PHI Involved i.e., if PHI is more "sensitive" nature. If credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud are involved, this *cuts against* finding "low probability" that PHI was compromised. With clinical information, consider nature of the services, as well as the amount of information and details involved.
Unauthorized Person who used the PHI or to whom the disclosure was made.	Consider who the unauthorized recipient is or might be. If the recipient person is someone at another CE or BA, then lower the probability that the PHI has been compromised since such entities are obligated to protect the privacy and security of PHI in a similar manner as the CE or BA from where the breached PHI originated. Compare to if PHI was impermissibly disclosed to their employer who could compare information against dates of absence from work.

"LOW PROBABILITY" PHI COMPROMISED

Four (4) Factors (Risk) Assessment

Whether the PHI was actually Acquired or Viewed.	Consider if the PHI was actually acquired or viewed or, rather, only the opportunity existed i.e., if the CE/BA mails the information to the wrong individual who opens the envelope and calls the CE/BA to say that he/she received the information in error. HHS points out that in such a case, the unauthorized recipient viewed and acquired the information because he/she opened and read the information and so this cuts against a finding that there is a low probability that the PHI was compromised. To contrast, if a laptop computer was/is stolen and later recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, could determine that the information was not actually acquired.
Mitigation – the extent to which the risk of the PHI has been mitigated.	A CE or BA *must* attempt to mitigate the risks to PHI following any impermissible use or disclosure, such as by obtaining the recipient's **satisfactory assurances** that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. When determining the probability that the PHI has been compromised, CE or BA should consider the **extent of what steps needed to be taken to mitigate, and how effective the mitigation was.**

Breach Reporting Requirements

Federal Breach Reporting Requirements

Number of Individuals Affected by the Breach	Federal: Office of Civil Rights (OCR)
Less than 500 individuals	Annually. Filing / reporting of breaches are due to the DHHS/OCR no later than 60 calendar days after the end of the calendar year in which the breach occurred. Go to link: http://ocrnotifications.hhs.gov/
500 individuals and above	•Without unreasonable delay and in no case later than 60 calendar days following a breach at http://ocrnotifications.hhs.gov/ •Notify the Media outlets serving the State or jurisdiction (e.g., in the form of a press release).

BA Breach Notification to Care1st

Under the Business Associate Agreement between Care 1st and its BAs:

- BAs must notice Care1st within 10 business days of discovery if the breach pertains to unsecured PHI; all other compromises (or attempts) within 20 business days.

- If BA is an *Agent* of Care1st, BA must ***immediately***, but no later than 1 business day of discovery, report the breach to Care1st. All other compromises (or attempts) within 10 business days.
  - "*Agent*" is determined in accordance with the federal common law of agency.

Breach Notification Timeframe Requirements to Members

Member Breach Notification Timeframes Requirements

Number of Individuals Affected by the Breach	Care1st Notification to Members:
Less than 500 individuals	Without reasonable delay and in no case later than 60 calendar days following the discovery of a breach.
500 individuals and above	Same

Questions? Ask us or look online.

- Care1st Compliance Department (602) 474-1377
- Care1st Compliance Department email @ ComplianceDepartmentAZ@care1stAZ.com
  - Remember: do not send any unsecure emails containing PHI.
- Care1st's HOTLINE Number @ 1-866-364-1350
- Visit http://www.hhs.gov/ocr/privacy/index.html