Healthcare Breach Management: Business Associate Agreement Addendum

By Beth Hjort, RHIA, CHPS and Harry Rhodes MBA, RHIA, CHPS, CPHIMS, FAHIMA

January 22, 2010

Healthcare contractual relationships between covered entities (CE) and business associates (BA) changed February 17, 2009 when the American Recovery and Reinvestment Act of 2009 (ARRA) regulated HIPAA's privacy and security rules applicable to business associates just as for covered entities. The Act enacts the extension of certain sections of the Privacy and Security Rules to business associates as of February 17, 2010. With breach notification requirements added simultaneously, the changes urge BAs and CEs to revisit, reposition and coordinate communication and work process understanding to meet the new regulations. The changes affect BAs and CEs engaged in outsourced activities involving protected health information (PHI) addressed in business associate agreements (BAA). These breach notification provisions are found in section 13402 of the Act and apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information.

AHIMA recognizes the urgency and challenges posed to both stakeholders particularly for breach notification compliance and has prepared this article and template contractual breach management addendum language for use as a starting point in BAA negotiations. It addresses considerations for a collaborative approach to expedite and smooth operational wrinkles as federal regulatory compliance is accomplished under the guidance of a healthcare organization's legal counsel. The guidance provided herein is not intended to address the specialized business relationship of 'agent'. Legal guidance is likewise encouraged in such circumstances.

At any given time, covered entities may support a large number of business associate agreements, each with customized activities, processes and expectations. Likewise, business associates may be partners with a large number of covered entities and operating under different business associate agreements, each of these agreements will different. At least two viewpoints have emerged from analysis of the ARRA law as to the necessity of updating BAAs. At a minimum AHIMA recommends the agreements be reviewed by the covered entity as the party originating the protected health information involved in the activities associated with the agreement. The decision to update an existing agreement or not is one advised be made under oversight of the CE's legal counsel based on a particular agreement's conditions. A CE may

---

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

choose to retain or add to existing agreements, general contract terms such as 'the business associate will comply with "all present and future laws and regulations". The guidance that follows in this article has been prepared to assist those who do choose to modify the BAA to address the breach management coordination including breach notification processes obligated by the new HHS regulations.

If modifying BAAs to address breach notification management advise inclusion of:

Effective breach notification compliance is a coordinated, shared responsibility though the CE holds the greater responsibility as primary custodian of the data; BA and CE Breach notification obligations are found in ARRA section 13402 of the Health Information Technology for Economic andClinical Health Act (HITECH) Notification in the Case of Breach of the Act. The necessity for a formal coordinated response that clearly spells out the shared CE/BA responsibility is even more significant considering the limited timeliness requirements entities are under to respond to a breach. Section 164.404 of the interim final rule, released by the HHS Office of Civil Rights (OCR) and effective September 23, 2009, provides the requirements for the notifications affected entities are to provide to individuals affected by a breach of unsecured protected health information. Section 164.404 includes implementation specifications regarding timeliness, content, and methods of the notice.

In order to avoid confusion all terminology referred to the business associate agreement should be in compliance with approved definitions. Clear understanding of defined terms in the agreement will ensure compliance.

Business Associate as an agent of the CE: The BA is considered an agent in situations where the BA has fiduciary authority to take independent action on behalf of the CE. A formal definition for agent is provided in the Federal common law of agency. If the BA is considered an agent the breach imputed to CE and the 60 day breach notification period begins with discovery.

Business Associate as independent contractor of the CE: The BA designated as an independent contractor will have access to the CE's PHI; but has no fiduciary authority to take independent action on behalf of the CE. If the BA is considered to be an independent contractor the 60 day breach notification period begins with notification of CE. In situations where there the BA is considered to be an independent contractor the notification timing in BA contracts the notification timing in BA contracts would need to be Revised to require the BA to provide the CE with immediate notification of breach. Timelines would also need to be negotiated regarding follow up with detailed information about individuals impacted by the breach.

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

Protected Health information (PHI) is defined on page 42740, column 3 of the Federal Register / Vol. 74, No. 162 / Monday, August 24, 2009 / Rules and Regulations (see references below) citing HIPAA's privacy rule: The HIPAA Privacy Rule defines protected health information as the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions. PHI covered in the ARRA regulations pertains to any medium of PHI as addressed in HIPAA, electronic, paper and verbal.

A definition of a breach is defined on page 42740, column 3 of the Federal Register / Vol. 74, No. 162 / Monday, August 24, 2009 / Rules and Regulations] Section 13400(1)(A) of the Act defines ''breach'' as the ''unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.''

Unsecured protected health information (PHI): The Act at section 13402(h) defines ''unsecured protected health information'' to mean PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance. The BAA should state that both parties have a responsibility to monitor for any issued guidance.

Wording in the business associate agreement must clearly delineate roles and responsibilities. The following is recommended.

CE and BA Obligations. The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA)Section 13402 (page 42740, Column 3 of the Federal Register / Vol. 74, No. 162 / Monday, August 24, 2009 / Rules and Regulations) addresses who must be prepared to comply with breach notification regulations: "HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information (PHI)."

Business Associate defined: ARRA points to HIPAA's definition in 45 CFR 160.103 (page 42740, column 3 of the Federal Register / Vol. 74, No. 162 / Monday, August 24, 2009 / Rules and Regulations) when defining a business associate "…a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information."

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

Covered Entity defined: The Act incorporates the definitions of ‘‘covered entity,’’ used in the HIPAA Administrative Simplification regulations (45 CFR parts 160, 162, and 164) (HIPAA Rules) at § 160.103. Under the HIPAA Rules, a covered entity is a health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan.

Standardized Security processes & procedures: The business associate agreement should set an expectation for the establishment of an ongoing security program in line at a minimum with that specified in the HIPAA Security Rule. The security administration activities should be in place to assess, monitor, prevent and mitigate security threats. Should the security administration activities uncover information breaches a formal response must be immediately implemented.

The security administration program should include a proper risk assessment**:**

- Asset inventory and prioritization
- Identify threat and vulnerability
- Review existing security controls
- Determine likelihood of exposure
- Determining the impact of a security breach
- Prioritize & mitigate identified risks
- Establish a Security Incident Response Team

A formal plan of action for a potential breach should include an audit plan, harm threshold, response triggers, communication protocol, chain of command, contact information and back up contact information for key responsible parties at BA and CE, education, training, mitigation process, breach notification timeliness, content, and methods of the notice. The business associates security administration should be in compliance with the covered entities security administration program and approved by the covered entity.

Encryption of unsecured protected health information: The BA shall upon the request of the CE employ technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals that are consistent with National Institute of Standards and Technology (NIST) Special Publications Available at *http://www.csrc.nist.gov/* If the BA has an established encryption process and methodology the BAA should require its utilization. The BA and CE shall jointly commit to establishing the necessary encryption technical requirements to allow for the secure exchange of encrypted PHI.

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates’ products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

BA exercises reasonable diligence; The BA must have in place reasonable systems for discovery of breaches. (Page 42749 the Federal Register / Vol. 74, No. 162 / Monday, August 24, 2009 / Rules and Regulations)

Workforce training and education; The BA shall ensure their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so. The BAA shall also commit the CE to providing CE workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so. Furthermore, the CE shall assist the BA in training their workforce members and other agents on specific or unique CE processes,

Timing of breach discovery and reporting: Business Associates shall treat all breaches as discovered and report the breach to the CE the first day known or should have been known by a BA exercising due diligence. There is an expectation of breach discovery if the BA is exercises due diligence, in such circumstances the expectation is that the BA should have known. The BA shall be required to report potential breaches to the CE on the first day known or should have been known by a BA exercising due diligence. The BAA should allow the CE to set a time limit on the number of days between discovery of a potential breach and the reporting of the breach to the CE.

Breaches Treated as Discovered – As delineated in the breach notification provisions of Section 164.404(a)(2) of the HIPAA Privacy Rule a breach shall be treated as discovered by a BA as of the first day the breach is known to the BA, or by exercising reasonable diligence would have been known to the BA. Thus, a BA is not liable for failing to provide notification in cases in which it is not aware of a breach unless the covered entity would have been aware of the breach had it exercised reasonable diligence.
Section 164.404(a)(2) further provides that a covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity

Because a covered entity or business associate is liable for failing to provide notice of a breach when the covered entity or business associate did not know—but by exercising reasonable diligence should have known—of a breach, it is important for the business associate agreement to required implementation of reasonable systems for discovery of breaches.

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

BAA obligation begins at the discovery of a breach and continues as long as related activity continues, until all effects of the information breach are mitigated. Because the potential for private right of action exists the business associate agreement should address the obligations of all parties. The BAA must address all points of collaboration supportive of efficient resolution. The BAA should establish agreed upon mitigation timelines as well as clearly stated responsibilities with regard to breach notification and mitigation.

Designated a point person: The BAA shall designate and provide a point of contact as well as applicable phone numbers, e-mail address, and other contact information both on and off business hours and back up point of contact for the CE and BA. The designated point person could be the staff member serving as the entities privacy official.

Meeting CE Compliance Requirements: Matters pertaining to PHI privacy and security shall be resolved to the satisfaction of the CE Compliance requirements.

Performance of Risk Assessment: The BA shall be expected to complete or participate in an investigation/risk assessment following a suspected information breach;

Immediately following a suspected security breach the CE and BA shall collaborate on the performance of a risk assessment to determine if an impermissible use or disclosure of protected health information constitutes a possible information security breach. The objective of the risk assessment shall be to determine if a significant risk of harm to the individual exists as a result of the impermissible use or disclosure. The risk assessment shall determine is a harm threshold has been crossed and there exists a significant risk of financial, reputational, or other harm to the individual.

Should the risk assessment result in a determination that individually identifiable protected health information held by the BA has been breached and a significant risk of financial, reputational, or other harm to the individual exists; the BA shall corroborate with the CE to notify the affected and individuals and mitigate the negative impact of the breach. Working with the CE the BA shall;

1. Notify CE immediately [defined in contract] upon discovery; The BA shall support the CE 60-day notification Compliance requirements by reporting suspected PHI security breaches immediately upon discovery.
2. Corroborate with the CE on breach risk assessment and investigation: The BA and CE shall commit necessary and appropriate staff and resources to the Security Incident Response

---

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

Team and Harm Threshold Assessment process to ensure compliance with mandated timelines.

3. Commit to expeditious responses and workflow turnaround. The BA shall commit the resources and staff necessary to ensure compliance with mandated timelines.
4. Participate in Notification Process: The BA shall be involved in the breach notification process; the BA may be delegated part or all of the notification process if appropriate, especially if it has been determined that responsibility for the breach rests with the BA.
5. Deliver indemnification statement: The BA shall indemnify the CE, against any and all liability and reasonable expenses actually and necessarily incurred by CE in connection with the defense or settlement of any action, suit or proceeding in which it is determined that financial, reputational, or other harm is inflicted upon an individual and the BA is adjudged in such action, suit or proceeding to be guilty of or liable for willful misconduct in the performance of duty and as to such matters as shall be settled by agreement predicated on the existence of such liability. The BA accepts responsibility for their actions and agrees to indemnify or compensate the CE for any claims against it that are the result of the BA's actions or inactions
6. Determine if financial incurrences rest with responsible party: Should it be adjudged that the BA is at fault for financial, reputational, or other harm is inflicted upon an individual as the result of an impermissible use, identity theft, or disclosure of PHI all associated costs are the responsibility of the BA.
7. Notify the Media involving multiple Covered Entities: In business cases where a PHI breach occurs at a business associate involving the protected health information of multiple covered entities. The CE involved would only be required to provide notification to the media if the information breached included the protected health information of 500 or more individuals located in any one State or jurisdiction. However if the business associate discovers that breach involves PHI from multiple covered entities and the entities involved are unable to determine which entity's protected health information was involved. The CE reserves the right to direct the business associate to take responsibility for administrating the breach notification process including the notification of the media in cases where the PHI of 500 or more individuals. The CE retains the right to oversee the process by which the media is notified. Additionally, in such cases where the entities involved are unable to determine which entity's protected health information was involved in the PHI breach the BA shall have the obligation of notifying the Secretary under § 164.408(b) concurrently with notice to the affected individuals; however, both covered entities must include this breach in their annual submission to the Secretary pursuant to § 164.408(c).

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

Business Associate Subcontractors: The BA shall ensure that provisions of the business association agreement are contained in the business associate agreement of all subcontractors that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information (PHI).

REFER TO: HOW TO REACT TO A SECURITY INCIDENT SIDEBAR: BE PREPARED TO COMMUNICATE WITH THE MEDIA, ALSO DESIGNATING A COMMUNICATIONS COORDINATOR BY NANCY DAVIS:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_036247.hcsp?dDocName=bok1_036247#communicate

Resources:
AHIMA Practice Brief: Letters of Agreement and Contract 2003
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_018254.hcsp?dDocName=bok1_018254

How to Handle a Security Incident – BA Requirements spelled out?
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_036247.hcsp?dDocName=bok1_036247

H.R.1 American Recovery and Reinvestment Act of 2009 (http://thomas.loc.gov)

45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule (http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf)

13402(f) Notification in the Case of Breach, Content of Notification (http://thomas.loc.gov)

Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt)

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.

45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

45 CFR Parts 160 and 164 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

This practice guidance addresses HHS breach notification regulations considerations for contractual relationships between covered entities and business associates. It does not address non-CE business associates' products and services such as PHRs. For regulatory compliance guidance, the reader is directed to 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf The user is further alerted that breach notification cases involving HIPAA covered entities and business associates defaults to HHS for compliance management 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule Page 42743.