Guidelines for a Compliant Business Associate Agreement - Retired

Save to myBoK

This 2013 practice brief version has been retired and is retained here for historical purposes. Read the 2016 updated version of this Practice Brief here.

The Privacy Rule portion of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines a "business associate (BA)" as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity (CE)."[1] The rule requires that a covered entity obtain satisfactory assurance in writing—in the form of a contract or other agreement—from their business associates of their commitment to appropriately safeguard PHI. Such assurances safeguard the PHI obtained, created, or received on behalf of the CE in the performance of the BA's duties for the CE. The rule excludes from the definition of BAs the CE's own workforce. However, a covered healthcare provider, a health plan, or a healthcare clearing house could be a BA of another CE.[2]

On January 25, 2013, the US Department of Health and Human Services (HHS) published the final Omnibus Rule which expands the provisions of HIPAA brought forth in the Health Information Technology for Economic and Clinical Health Act (HITECH). The sections affected by these changes include privacy, security, enforcement, and breach

The final Omnibus Rule expanded the definition of a business associate to include subcontractors that create, receive, maintain, or transmit PHI on behalf of another BA.[3] The definition of the term BA was also expanded to include:

- Health information organizations
- E-prescribing gateways
- A person that provides data transmission services for PHI exchange on behalf of a CE and requires access to such information on a routine basis
- Personal health record (PHR) vendors

In order to be compliant, covered entities and their BAs should review their BA agreements with the new requirements imposed by the Omnibus Rule provisions as follows:

- Security Standards (45 C.F.R. § 164.306)
- Administrative Safeguards (45 C.F.R. § 164. 308)
- Physical Safeguards (45 C.F.R. § 164.310)
- Technical Safeguards (45 C.F.R. § 164.312)
- Organizational Requirements (45 C.F.R. § 164.314)
- Policies and Procedures (45 C.F.R. § 164.316)
- Notification to the Secretary (45 C.F.R. § 164.410)
- General Rules; Uses and Disclosures of PHI (45 C.F.R. § 164.502)
- Organizational Requirements; Uses and Disclosures (45 C.F.R. § 164.504)

The rule now allows a BA to disclose PHI to their subcontractors when they enter into a BA agreement with them. The BAs are responsible and liable to the CE for the activities of their subcontractors who have entered into a BA agreement with them. If a BA's contractor becomes aware of a violation of its contractual BA agreement, it must take steps to cure the breach or terminate the agreement if resolution is unsuccessful.

The Privacy Rule's BA contract provision sets the requirements that should be addressed by the BAs. The Office for Civil Rights (OCR) also provided a model BAs agreement on its website for or use by covered entities.[4] The modifications to the HIPAA Privacy and Security Rules exempt covered entities from enforcing contractual violations of its BAs agreements.

Instead the HHS may now directly enforce privacy and security rule violations by BAs in the same manner as CE violations. This makes HIPAA's criminal and civil penalties applicable to BAs.

Compliance Date for the Omnibus Rule

Business Associate Agreement (BAA) compliance dates vary as follows:

- If there is an existing agreement between a covered entity and its business associate that has been signed prior to January 25, 2013 (the date of publication of the Omnibus Final Rule) and does not need to be renewed by March 26, 2013 or September 23, 2013, then the agreement can remain valid until September 23, 2014. This effectively created a transition period of one year from the compliance date of September 23, 2013.
- If the BAA was executed after January 25, 2013, then it must be compliant with the Omnibus Rule by September 23, 2013.

Components of the Business Associate Agreement

The components of a Business Associate agreement are:

1. Parties to the BA agreement (CE and BA; BA and subcontractor of the BA)
2. Purpose of the BA agreement (compliance with HIPAA and HITECH)
3. Definitions:

    a. Breach
    b. Electronic PHI
    c. Individual
    d. PHI
    e. Law
    f. Secretary
    g. Security incident

4. Obligations and activities of the BA (or subcontractor)

    a. Use and disclosure
    b. Appropriate safeguards
    c. Reporting (of inappropriate disclosures/breach)
    d. Mitigation
    e. Agents (subcontractors or staff of BA)
    f. Access to PHI
    g. Amendments to PHI
    h. Access to books and records
    i. Accounting of disclosures
    j. Patient restriction for restrictions and confidential communications

5. Permitted uses and disclosures by BA (or subcontractor)

    a. As required by CE as defined in the services being provided by BA for CE or services being provided by the subcontractor for the BA
    b. Use for administrative activities of the BA or subcontractor
    c. Disclosure as required by law

6. Term and termination

    a. Term of BA agreement
    b. Termination of BA agreement for cause
    c. Effect of termination

i. Return or destruction of PHI
ii. Provision for satisfying HHS requirement of BA to retain records for four years
iii. Adequate protections of retained PHI

7. Indemnity for both parties
8. Miscellaneous

    a. Regulatory references
    b. Survival after termination of BA agreement
    c. Governing law
    d. Entire agreement language

9. Signatures, titles, and dates of agreement execution by the parties

Vetting Process for BA, Ensuring HIPAA/HITECH Compliance

BAs must have a comprehensive program to ensure the covered entities information is properly protected. The BA must have a carefully constructed set of privacy and security policies and procedures. These policies and procedures should be reviewed by the CE as part of the contracting process. Policies should cover employees, volunteers, contractors, and other members of the BA workforce, as defined by HIPAA.

The policy and procedure set should include, at a minimum, the following:

- Privacy and security official designations
- Access controls and appropriate security safeguards
- Minimum necessary provisions
- Sanction Policy
- Breach notification
- Workforce training and awareness programs for security and privacy
- Uses and disclosures of PHI
- Comprehensive security risk analyses
- Data retention
- Accounting of disclosures (if applicable)
- Patient requests for restrictions and confidential communications
- Risk assessment, risk management, access controls

Establishing an Ongoing Security Program

Through the agreement, the CE should set an expectation that the BA maintain an ongoing security program that should at a minimum align with requirements specified in the HIPAA security rule. The BA should have in place security administration activities to assess, monitor, prevent, and mitigate security threats. The BA's security administration should be in compliance with the CE's program and approved by the CE. The program should include reasonable systems for discovery of breaches and a formal response plan should a possible breach be discovered.

As part of its risk analysis activities, the BA should:

- Inventory and prioritize assets
- Identify threats and vulnerabilities
- Review existing security controls
- Determine the likelihood of exposure
- Determine the impact of a security breach
- Prioritize and mitigate identified risks
- Establish a security incident response team

The plan of action for a potential breach should include breach analysis and determination led by the CE with the assistance of the BA. The plan of action should include: an audit plan, four step risk assessment, response triggers, communication protocol, chain of command, contact information, education, training, mitigation process, breach notification timeliness, content, methods of the notice, and back-up contact information for key responsible parties at the BA and CE.

A four step risk assessment for breach determination should include:

- The **nature and extent** of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The **unauthorized person** who used the PHI or to whom the disclosure was made
- Covered entities must determine whether or not the **PHI was actually acquired or viewed** or whether there was an opportunity for the PHI to be acquired or viewed
- The **extent to which** the risk to the PHI **has been mitigated**

The BA should ensure that provisions of the BA agreement are contained in the agreements it holds with its subcontractors that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.

Encryption

Under the regulation, a breach occurs only when PHI is unsecured. For this reason, CEs may consider requiring that the BA employ technologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals that are consistent with guidance from the National Institute of Standards and Technology and OCR.

The BA and CE shall jointly commit to establishing the necessary encryption technical requirements to allow for the secure exchange of encrypted PHI.

Workforce Training and Education

With the HIPAA Omnibus final rule, BAs are required to train their workforce on HIPAA privacy and security awareness. The BA agreement may request confirmation that BA 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 BA agreement can also commit the CE to ensuring its own workforce members and agents receive similar training and awareness. Furthermore, the CE can assist the BA in training workforce members and other agents on specific or unique CE processes. The CE can require the BA workforce to attend and complete the CE's training.

Consider the following example. Hospital A has a BA agreement with Coding Company B. Coding Company B has vendors and subcontractors that do data destruction, backlog coding, and other related services. These subcontractors could be required to attend Hospital A's HIPAA privacy and security training.

Contingency Operations

The CE may request a copy of the contingency plan from the BA. The contingency plan should include details on the backup and disaster recovery processes.

Security Compliance, HIPAA Violation Detection and Reporting

Covered entities are required to assess and monitor their business associate HIPAA security and privacy compliance programs. Through BA agreements and other legal instruments, CEs mandate that BAs implement appropriate physical, technical, and administrative safeguards. These safeguards are meant to prevent unauthorized access, use or disclosure of PHI, including implementing requirements of the HIPAA security rule with regard to electronic PHI. They must also require the BA to ensure that any sub-contractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the BA with respect to such information.

BAs and BA sub-contractors must perform security and privacy risk analysis to document the areas where they are in compliance with HIPAA rules and areas where mitigation is needed. Security and privacy risk analysis should be undertaken on a routine basis in order to prioritize risks, determine mitigation priorities, and reduce risks to an acceptable level. These prioritized risks will become a part of the CE and BA global risk management plans. These are ongoing processes, which require continued assessment as computer networks and systems change. These analyses should be reviewed and reassessed yearly to ensure full compliance.

Many times BA agreements are meant to work in conjunction with master agreements between a CE and BAs. The master agreement is the original business agreement between a CE and BA. Any of these agreements may delineate additional privacy and security safeguards and monitors.

Sometimes these are listed as blanks in the BA agreement or master agreement templates, which are filled in for each different BA. Specifics adopted by the CE can be incorporated into the template itself as well.

BA agreements shall be documented and maintained—as shall be all documentation used for HIPAA compliance in regards to the BAs or sub-contractors, according to the HIPAA documentation policies—for a minimum retention period of 6 years.

HIPAA Violation and Breach Discovery

CEs and BAs must agree upon potential HIPAA violation and breach discovery timeframes. They must determine the roles the the CE and BA will assume in the event of possible HIPAA violation investigation, violation and breach determination, and breach notification processes.

Under the HIPAA Omnibus Final Rule, CEs, BAs, and subcontractors are all directly liable for HIPAA compliance. Typically both the CEs and BAs will employ a defined procedure for determining when a discovered incident or event has occurred that may be deemed either a privacy or security violation or a breach as generally outlined by the following steps:

- Investigation and documentation by the BA of a privacy or security incident or event
- Reporting mechanisms and timeframes by the BA to the CE of the discovered incident or event
- HIPAA violation and breach determination by the CE and BA
- Breach notification (by the CE or BA) as governed by the agreements
- Appropriate actions including mitigation, remediation, and sanctions to resolve the breach incident
- Feedback, mitigation, sanctions, and corrective actions developed and recorded provided by the BA or subcontractor

Establishing a System for Discovery of Breaches

HHS's has previously defined a breach as a use or disclosure that "compromises the security or privacy of the PHI," which means to pose "a significant risk of financial, reputational, or other harm to the individual." To determine if an impermissible use or disclosure of PHI constitutes a breach, covered entities and BAs will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. The burden of proof is on the CE or BA and the responsibilities should be clearly defined in the BA agreement. Subcontractors that work on behalf of a BA and handle PHI are required to comply with the applicable privacy and security rule provisions and are subject to the same liability for failure to do so.

The rules now assume that any impermissible use or disclosure of PHI constitutes a breach. This implies that notification is necessary in every situation except when a CE or BA determines that there is a low probability that the PHI has been compromised. There are some instances of violations that are considered to be low risk and thus are exempt from the breach notification requirements. These are:

1. A workforce member unintentionally accesses or uses PHI in good faith
2. An inadvertent disclosure between two authorized individuals to access PHI at the same CE, BA, or organized healthcare arrangement
3. Disclosures where the CE has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI

After an impermissible use or disclosure, covered entities and BAs must either notify the individuals or perform a risk assessment and determine if breach notification is needed. The risk assessment must cover:

- The nature and extent of PHI involved
- The unauthorized person who used the PHI or to whom it was disclosed
- Whether the PHI was actually acquired or used
- The extent to which the risk was mitigated

A breach only occurs if it involves unsecured PHI. Covered entities and BAs are encouraged to take advantage of the safe harbor provision of the Breach Notification Rule by the use of encryption and secured data sets. BAs are strongly advised to comply with the guidelines detailed in the Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals section of the breach notification interim final rule. If PHI is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.

For further guidance on breach notification for unsecured protected health information consult AHIMA's Practice Brief that appeared in the September 2013 *Journal of AHIMA*, Performing a Breach Risk Assessment.

Notes

1. Department of Health and Human Services' Office for Civil Rights. "Business Associates." April 3, 2003. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.
2. Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." *Federal Register*. 45 CFR Parts 160 and 164. January 25, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
3. Department of Health and Human Services' Office for Civil Rights. "Business Associate Contracts." January 25, 2013. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
4. Ibid.

References

AHIMA. "Performing a Breach Risk Assessment." *Journal of AHIMA* 84, no. 9, (Sept 2013): 66-70.

Department of Health and Human Services. "Breach Notification for Unsecured Protected Health Information." *Federal Register*. 45 CFR Parts 160 and 164. August 24, 2009. http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf.

Department of Health and Human Services. "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." *Federal Register*. 45 CFR Parts 160 and 164. April 27, 2009. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

Hjort, Beth and Harry Rhodes. "Putting It in Writing: Updating BA Agreements to Cover Breach Notification." *Journal of AHIMA* 81, no.6 (June 2010): 52-53.

National Institute of Standards and Technology. NIST SP 800-111, Encryption Guidance. http://www.csrc.nist.gov.

North Carolina Healthcare Information and Communications Alliance, Inc. "Business Associate Agreement." March 22, 2013. http://www.nchica.org/HIPAAResources/Reviewed.htm.

Prepared by

Barbara Beckett, RHIT, CHPS
Kathy Downing, MA, RHIA, CHP, PMP
Rose Dunn, MBA, RHIA, CPA, FACHE
Susan Lucci, RHIT, CHPS, CMT, AHDI-F
Kelly McLendon, RHIA, CHPS
Godwin Odia, PhD, NHA, RHIA
Harry Rhodes, MBA, RHIA, CDIP, CHPS, CPHIMS, FAHIMA
Mariela Twiggs, MS, RHIA, CHP, FAHIMA

Appendix A—AHIMA Model Language: Business Associate Agreement

Any access, use or disclosure of PHI for non- Treatment, Payment, or Operations reasons must be pursuant to a signed patient (or their representative) written authorization.

Prior to implementing this business associate agreement, consultation with your legal counsel is paramount.

The following model Business Associate Agreement language does not constitute a contract in and of itself. This document represents a vetted compilation based upon an environmental scan of business associate agreement models and best practices and has been created as a specimen for example purposes. Each Business Associate Agreement, (BAA) is unique to the organization and setting and should only be adopted after careful vetting, adaptation and endorsement by Legal Counsel. AHIMA makes no warranties express or implied in offering this model sample language for use.

This Business Associate Agreement (the "Agreement") between <insert CE name> hereinafter referred to as "Covered Entity" or "CE", and <insert BA name>, hereinafter referred to as "Business Associate."

RECITALS

1. The identified Covered Entity desires to disclose certain health information to Business Associate pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI") (defined below).
2. Covered Entities and Business Associates propose to ensure confidentiality, protect the privacy, and provide for the security of PHI disclosed to Business Associate pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws. The Health Information Technology for Economic and Clinical Health ("HITECH") Act of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, modified the HIPAA Privacy and Security Rules (hereinafter, all references to the "HIPAA Privacy and / or Security Rules" include all amendments thereto set forth in the HITECH Act and any accompanying regulations).
3. A component of the HIPAA Regulations, the Privacy Rule (defined below) mandates the Covered Entity to execute a contract containing express requirements with Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.502(e) and 164.504(e) of the Code of Federal Regulations ("CFR") and contained in this Addendum.

Upon reflection for the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

Definitions

Catch-all definition:

The source for the following common definitions used in this Agreement shall be the glossary of terms published in the HIPAA Privacy and Security Breach Notification, and Enforcement Rules: Breach, Data Aggregation, Designated Record Set,

Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Agent. "One who represents and acts for another under the contract or relation of agency Source: Black's Law Dictionary.

Breach: Under HITECH, the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part that compromises the security or privacy o the protected health information (45 CFR 164.402 2013)

Breach notification: As amended by HITECH, a covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach (45 CFR 164.404 2013)

Protected health information (PHI): As amended by HITECH, individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years (45 CFR 160.103 2013)

(b) Business Associate. For purposes of this agreement, business associate includes all agents and subcontractors. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(c) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(d) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Business Associate Obligations and Activities

Business Associate agrees to:

Permitted Uses

Business Associates agree to only use or disclose protected health information in compliance with and as permitted or required by the Agreement or as required by law.

Permitted Disclosures

A Business Associate or its agents or subcontractors shall not disclose Protected Health Information in any manner that would constitute a violation of the Privacy Rule if disclosed by CE, except that Business Associate may disclose Protected Health Information (i) in a manner permitted pursuant to the Agreement and Addendum,; (ii) as required by law, and, with the prior written approval of CE which may be granted or withheld at CE's sole discretion either (iii) for the proper management and administration of Business Associate as reasonably determined by Business Associate in good faith or (iv) for Data Aggregation purposes for the Health Care Operations of CE. To the extent that Business Associate discloses Protected Health Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from such third

party that such Protected Health Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) an agreement from such third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Health Information, to the extent it has obtained knowledge of such breach. Any access, use or disclosure of PHI for non- Treatment, Payment or Operations reasons must have be pursuant to a signed patient (or their representative) written authorization. See for reference 45 CFR §164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii).

Appropriate Safeguards

Business Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by this Agreement. Business Associates shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities and implement reasonable and appropriate policies and procedures in order to comply with the standards, implementation specifications, and other requirements of the Privacy Rule. Business Associate shall maintain a written (which may be electronic) record of any action, activity, or assessment under such policies and procedures. Business Associate shall change or amend its policies and procedures as necessary and appropriate to comply with changes in state and federal law, and shall promptly document and implement the revised policy or procedure. Business Associate shall implement the administrative, physical, and technical safeguards set forth in Sections 164.308, 164.310, and 164.312 of the HIPAA Privacy and Security Rules that reasonably and appropriately protect the confidentiality, integrity, and availability of any Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and, in accordance with Section 164.316 of the HIPAA Privacy and Security Rules, implement and maintain reasonable and appropriate policies and procedures to enable it to comply with the requirements outlined in Sections 164.308, 164.310, and 164.312.

Notification of Breach, Mitigation & Report of Inappropriate Use or Disclosure

Business Associates agree to report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The Business Associate Agreement may provide specific guidance or instructions regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

Business Associate, Agents, or Subcontractors

In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associates shall ensure that any agents, including subcontractors, to whom it provides Protected Health Information agree in writing to create, receive, maintain, or transmit protected health information on behalf of the business associate in compliance with the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

Access to Protected Health Information

Business Associate shall make available protected health information in a designated record set maintained by Business Associate or its agents or subcontractors to Covered Entity (CE) for inspection and copying within five business (5) days of a request by CE to enable CE to satisfy covered entity's obligations under 45 CFR 164.524;

The Business Associate Agreement may provide specific guidance or instructions regarding how the business associate will respond to a request for access that the business associate receives directly from the individual.

(For example, instructions such as time and circumstances under which a business associate shall provide the requested access or the covered entity may retain the right to address the individual's access request.

Amendments to Protected Health Information

Within five (5) business days of a request by the CE, the Business Associate or its agents or subcontractors shall make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

The Business Associate Agreement may provide specific guidance or instructions regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual. (For example, instructions such as time and circumstances under which a business associate shall provide the requested amendment or the covered entity may retain the right to address the individual's amendment request.

Accounting of Disclosures

Within five (5) business days of notice by CE of a request for an accounting of disclosures of Protected Health Information, Business Associate and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR Section 164.528. In addition, the Business Associate and its agents or subcontractors maintain and make available the information required to provide an accounting of disclosures to either "covered entity" or "individual."

At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall within three (3) business days of a request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested.

[The Business Associate Agreement may provide specific guidance or instructions regarding how the business associate will respond to a request for accounting of disclosures that the business associate receives directly from the individual. (For example, instructions such as time and circumstances under which a business associate shall provide the requested accounting of disclosure or the covered entity may retain the right to address the individual's accounting of disclosure request.]

Government Access to Records

Business Associate and its agents or subcontractors shall make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules. Business Associate shall provide to CE a copy of any Protected Health Information that Business Associate provides to the Secretary concurrently with providing such Protected Health Information to the Secretary.

Minimum Necessary

Business Associate or its agents or subcontractors shall only request, use and disclose the minimum amount of Protected Health Information necessary to achieve the purpose of the request, use or disclosure; 45 CFR §164.514(d)(3). Until such time as minimum necessary guidance pursuant to the HITECH Act for purposes of the HIPAA Privacy and Security Rules is available, Business Associate or its agents or subcontractors shall, to the extent practicable, access, use, and request only PHI that is contained in a limited data set (as defined in Section 164.514(e)(2) of the HIPAA Privacy and Security Rules), unless Business Associate requires certain direct identifiers in order to accomplish the intended purpose of the access, use, or request, in which event

Business Associate may access, use, or request only the minimum necessary amount of Protected Health Information to accomplish the intended purpose of the access, use, or request. The information that constitutes the "minimum necessary" shall be determined by the CE based on the minimum amount need to accomplish its intended purposes.

Data Ownership

The Business Associate nor its agents or subcontractors shall hold any data ownership rights with respect to the Protected Health Information.

Retention of Protected Health Information

Throughout the term of the Agreement, Business Associate and its subcontractors or agents shall retain all Protected Health Information and shall continue to maintain the information and documentation thereof for a period of six (6) years from the later of (i) the date of its creation or (ii) termination of the Agreement. Business Associate shall review documentation periodically, and update as needed, in response to environmental and operational changes affecting the security of Protected Health Information. See for reference 45 CFR §164.530(j)(2) and 164.526(d).

Audits, Inspection and Enforcement

Upon written request by CE, the Business Associate and its agents or subcontractors shall within five (5) calendar days allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Health Information pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Agreement; provided, however, that (i) The Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing and location of such an inspection, (ii) The confidentiality of all sensitive proprietary information of Business Associate accessed by the CE during the course of the inspection shall be protected by the CE; and (iii) if requested by Business Associate a mutually agreed upon nondisclosure agreement shall be executed between the CE and the Business Associate. The fact that CE inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with this Agreement. The CE's (i) failure to detect or (ii) detection, failure to notify Business Associate, or require Business Associate's remediation of any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of CE's enforcement rights under this Agreement.

Privacy, Security, and Breach Notification Compliance Plan

During the term of this Agreement, Business Associate shall notify CE within five (5) days of any suspected, actual or Unauthorized Access to, Security Incident or other Breach of security or privacy, privacy event, improper or unauthorized use, intrusion and/or any actual or suspected use or disclosure of PHI in violation of this Agreement or any applicable federal or state laws, rules or regulations.

Furthermore, the Business Associate agrees to implement a necessary and appropriate comprehensive compliance plan and training program for the members of its workforce, agents, and subcontractors outlining the Privacy, Security, and Breach Notification Rules required to perform their workforce responsibilities.

Restrictions on certain disclosures of PHI

Business Associate agrees to comply with any requests for restrictions on certain disclosures of Protected Health Information to which Covered Entity has agreed in accordance with Section 164.522 of the HIPAA Privacy and Security Rules and of which Business Associate has been notified by Covered Entity. In addition, and notwithstanding the provisions of Section 164.522, Business Associate agrees to comply with an individual's

request to restrict disclosure of Protected Health Information to a health plan for purposes of carrying out payment or health care operations if the Protected Health Information pertains solely to a health care item or service for which Covered Entity has been paid by in full by the individual or the individual's representative and to which the Covered Entity has notified the Business Associate of in writing.

Remuneration for PHI

Business Associate agrees that it will not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual without the written authorization of the individual or the individual's representative, except where the purpose of the exchange is (i) for public health activities as described in Section 164.512(b) of the Privacy and Security Rules; (ii) for research as described in Sections 164.501 and 164.512(i) of the Privacy and Security Rules, and the price charged reflects the costs of preparation and transmittal of the data for such purpose; (iii) for treatment of the individual, subject to any further regulation promulgated by the Secretary to prevent inappropriate access, use, or disclosure of Protected Health Information; (iv) For the sale, transfer, merger, or consolidation of all or part of Business Associate and due diligence related to that activity; (v) For an activity that Business Associate undertakes on behalf of and at the specific request of Covered Entity; (vi)To provide an individual with a copy of the individual's Protected Health Information pursuant to Section 164.524 of the Privacy and Security Rules; or (vii) Other exchanges that the Secretary determines in regulations to be similarly necessary and appropriate.

Remuneration for written communication

Business Associate agrees that it will not directly or indirectly receive remuneration for any written communication that encourages an individual to purchase or use a product or service without first obtaining the written authorization of the individual or the individual's representative, unless: (i) such payment is for a communication regarding a drug or biologic currently prescribed for the individual and is reasonable in amount (as defined by the Secretary); or (ii) The communication is made on behalf of Covered Entity and is consistent with the terms of this Agreement. (iii) on and after February 17, 2010, Business Associate agrees that if it uses or discloses patients' Protected Health Information for marketing purposes, it will obtain such patients' authorization before making any such use or disclosure.

Secured vs. Unsecured PHI

For all PHI accessed, used and disclosed by the Business Associate efforts shall be made, as feasible, to create, manage, disclose and destroy all PHI which is controlled by the Business Associate in ways that meet the criteria established in 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 thereby yielding 'secured as opposed to 'unsecured' PHI which takes advantage of the safe harbor established that reduces the requirements for privacy Breach Notification. Faxes and paper copies of PHI are discouraged for all access, use and disclosure in favor of secured, according to the above definition, electronic access, use and disclosure.

Obligations of Covered Entity

Permissible Requests by Covered Entity

It shall not be permissible for a covered entity to ask a Business Associate, agent or subcontractor to utilize or disclose protected health information in any manner that would not be allowable under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

CE shall notify Business Associate as follows; i) of any changes in or revocation of permission by individuals to Use or Disclose their PHI, if such changes affect Business Associate's permitted or required Uses or Disclosures ii) of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to under 45 C.F.R. §164.522. iii) of any amendment to the PHI that Covered Entity has agreed to.

Business Associate Agreement Term and Termination

Term

The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

Termination for Cause

Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

Obligations of Business Associate upon Termination

[Option 1: If the business associate is to return or destroy all protected health information upon termination of the agreement. A certificate of destruction may be requested.]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2: If the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement. This arrangement would require an expressed written authorization from the CE. Upon termination of this extension to the original agreement, a certificate of destruction must be provided.]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

Judicial or Administrative Proceedings

Either party may terminate this Agreement, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

Survival

The obligations of business associate under this Section shall survive the termination of this Agreement.

Material Breach

A Breach by Business Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement by CE pursuant to Section 4c. See for reference, 45 CFR §164.504(e)(2)(iii).

Indemnification

Business Associate and its subcontractors or agents shall indemnify and hold CE harmless from and against any and all claims, liability, reasonable attorneys' fees and costs of suit arising out of or in connection with injuries or damages caused by Business Associate as a result of Business Associate's actions, conduct, behavior, malfeasance or negligence which result in Business Associate's failure to perform its duties and obligations under this Agreement.

Disclaimer

CE makes no warranty or representation that compliance by Business Associate and its subcontractors or agents with this Addendum, HIPAA or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

Amendment to Comply with Law

The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the Privacy Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Business Associate that Business Associate will adequately safeguard all Protected Health Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the Privacy Rule or other applicable laws. CE may terminate this Agreement upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by CE pursuant to this Section or (ii) Business Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the Privacy Rule.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. Additional regulatory reference(s) to sections in the HIPAA Rules that may affect or amend sections in the Business Associate Agreement.

(b) [Optional] Amendment. Necessary as needed amendments made for compliance with the requirements of the HIPAA Rules and any other applicable law entered into by mutual agreement of The Parties to the Business Associate Agreement

(c) [Optional] Interpretation. Any elucidation of ambiguity in the Business Associate Agreement made to ensure understanding and interpretation in compliance with the HIPAA Rules.

Addendum to Business Associate Agreement

This Addendum to the BAA sets forth additional terms attached to this document. This Addendum may be amended from time to time.

Addendum to Business Associate Agreement

This Addendum to the BAA sets forth additional terms attached to this document. This Addendum may be amended from time to time.

Additional Permitted Uses

Supplemental to those intents set forth in Section 2(a) of the Addendum, the Business Associate may use Protected Health Information as follows:

Additional Permitted Disclosures.

In addition to those purposes set forth in Section 2(b) of the Addendum, Business Associate may disclose Protected Health Information as follows:

Subcontractor(s) or Agents.

The parties to the BAA acknowledge that the subsequent list of subcontractors or agents of Business Associate shall secure Protected Health Information in the course of assisting Business Associate in the performance of its obligations under the Agreement and the Addendum:

Receipt.

Any receipt of Protected Health Information by the Business Associate and its agents or subcontractors pursuant to the Agreement and Addendum shall be deemed to occur as follows, and Business Associate and its

agent's or subcontractor's obligations under the Addendum shall commence with respect to such PHI upon such receipt:

Additional Restrictions on Use of Data.

Should the Covered Entity be a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, the Business Associate shall comply with the following restrictions on the use and disclosure of Protected Health Information:

(Optional) Monitors Used to Ensure Business Associate Compliance.

As a Covered Entity, the following monitors are utilized by our organization to ensure actions taken by the Business Associate and its agents or subcontractors are in compliance with HIPAA privacy and Security requirements:

(Optional) Safeguards Utilized Ensure Business Associate Compliance.

The following safeguards are utilized by this Organization as a Covered Entity to ensure Business Associate and its agents or subcontractors compliance with HIPAA privacy and Security requirements:

(Optional) Permitted De-identification.

Should the Business Associate be permitted to de-identify PHI according to HIPAA regulations, the Business Associate and its agents or subcontractors shall provide descriptions of the de-identified data set and the mechanisms utilized to perform the de-identification.

(Optional) Data Aggregation.

Should the Business Associate and its agents or subcontractors be permitted to aggregate PHI according to HIPAA regulations, these parties shall provide descriptions of the aggregated data set and the mechanisms utilized to perform the aggregation.

References

North Carolina Healthcare Information and Communications Alliance BAA Task Force. “Business Associate Agreement.” HIPAA Sample Documents. NCHICA BAA Task Force, March 22, 2013. http://www.nchica.org/HIPAAResources/Reviewed.htm.

Department of Health and Human Services. “Business Associate Contracts.” Published January 25, 2013. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Article citation:
AHIMA. "Guidelines for a Compliant Business Associate Agreement - Retired" (AHIMA Practice Brief, November 2013)