HIPAA Primer
Requirements for Business Associates

The Buck Stops Here for Business Associates Protecting PHI

By Mary Chaput, MBA, HCISPP, CIPP/US, CHP
CFO and CCO, Clearwater Compliance LLC
It’s not news. It’s been over ten years since the Health Insurance Portability and Accountability Act (HIPAA) required Covered Entities (CEs) to meet certain requirements related to protected health information (PHI) through compliance with the Privacy Rule. Effective 2015, CEs were required to implement protections under the Security Rule. In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act added new rules regarding Breach Notification and enforcement; and extended applicable compliance requirements directly to Business Associates (BAs) - those individuals or entities that perform activities involving PHI on behalf of CEs. Most recently, The HIPAA Omnibus Final Rule (OFR), with a required compliance date of September 23rd, 2013, brought the rules together, along with others, under a single compliance umbrella. The OFR added details and implemented significant changes called for in the HITECH Act; one of the most significant changes ropes BAs into the HIPAA corral. Below are the redline changes confirming the responsibilities of BAs for HIPAA-HITECH regulations as a result of the OFR:

**CFR 45 Part 160 Administrative Requirements § 160.102 Applicability.**

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

**CFR 45 Part 164 Subpart C – Security Rule § 164.302 Applicability.**

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

**CFR 45 Part 164 Subpart E – Privacy Rule § 164.500 Applicability.**

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

The ramifications of non-compliance, once the concern of CEs, are now the concern BAs and their subcontractors, and the pain of those ramifications have increased for all under OFR.

Two other Clearwater Compliance whitepapers will delve into the specific Privacy and Security regulations applicable to BAs, given the services provided. The focus of this paper is to identify those organizations responsible to comply, the terms of the legal agreements between them, enforcement activities underway and the ramifications of non-compliance.
So what constitutes a Business Associate ("BA")?

According to the regulations, a BA is a person (who is not a member of the covered entity’s workforce) or entity who creates, receives, maintains, or transmits protected health information on behalf of a covered entity ("CE").

CEs include (1) health plans, (2) health care clearinghouses and (3) health care providers (doctors, dentists, therapists, psychologists, pharmacists, etc.) that transmit any health information in electronic form in connection with a HIPAA-covered transaction.

So BAs are service providers that handle, on behalf of a CE, the following type of activities:

- claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or
- provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity where the provision of the service involves the disclosure of PHI from the covered entity, or from another business associate of such covered entity or arrangement, to the person.
- data transmission services organization, such as a health information organization or e-prescribing gateway, that requires access on a routine basis to PHI.
- personal health record offerings to one or more individuals on behalf of a CE.

Specific examples of BAs include, but are not limited to:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

And a BA is also a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another BA.

And by the way, a CE can be a BA of another CE.

Activities that do not, in and of themselves, define a BA:

- Disclosures by a CE to a health care provider concerning treatment of the individual.
- Certain disclosures by a group health plan to a plan sponsor.
- Disclosures to a government agency for determining eligibility or enrollment in a government public health plan.

To help clarify the definition of a BA and the need for BA contracts, HHS posted a list of situations in which a BA Contract is not required, either because the service provider is acting on its own behalf (and not on the behalf of the CE) or because the services provided are not regulated by the Administrative Simplification Rules:

- Incidental disclosures to persons or organizations (e.g., janitorial service
or electrician) whose functions or services do not involve the use or disclosure of PHI.

- For conduits, for example, the US Postal Service, certain private couriers (think FedEx and UPS), and their electronic equivalents, who have only “random or infrequent” access to PHI.xii

- Disclosures among CE participants in an organized health care arrangement (OHCA) that relate to their joint health care activities.

- Where a group health plan purchases insurance from a health insurance issuer or HMO.

- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer.

- To disclose protected health information to a researcher for research purposes, either with patient authorization or as a limited data set.

- When a financial institution processes consumer-conducted financial transactions that directly affects the transfer of funds for payment for health care or health plan premiums.

And the Privacy Rule allows for certain exceptions in situations where a CE is not required to have a BA contract in place before disclosing PHI to the person or entity:

- Disclosures for payment activities such as
  - Disclosure to a health plan to obtain premiums or determine or fulfill obligations for coverage or provision of health benefits
  - Disclosure by a provider to a health plan for payment activities for the provision of health care.xiii

- Disclosures between providers for treatment such as
  - From a hospital to a specialist to whom it refers a patient
  - From a physician to a laboratory
  - From a hospital laboratory to a reference laboratory.xiv

What’s needed in BA Contracts?

Prior to the HITECH Act, any BA of a CE with access to PHI was required to comply with the terms of a BA Agreement, which specified how the BA would handle and protect PHI, among other things. The HITECH Act placed the same obligation on subcontractors of BAs and the OFR added Privacy and Breach Notification requirements.xv The OFR also amended the Privacy Rule to specify that the CE is not responsible for obtaining assurances from the subcontractor of their BA.xvi

With the passage of the OFR, some additional elements (redlined below) were added to the contract requirements between the covered entity and a business associate:xvii

- Establish the permitted and required uses and disclosures of PHI
May not authorize the use or further disclosure in violation of the Privacy Rule

Provide that the BA will:

- Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic PHI;
- Report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information;
- Ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to these same restrictions and conditions;
- Make PHI available in accordance with an individual’s right of access;
- Make PHI available for amendment and incorporate approved amendments
- Make PHI available required to provide an accounting of disclosures
- To the extent the business associate is to carry out a CE’s obligation, comply with the Privacy Rule regulations that apply to the CE
- Make its applicable internal practices, books, and records available to the Secretary for purposes of determining the CE’s compliance with the Privacy Rule; and
- At termination of the contract,
  - if feasible, return or destroy all PHI received from, or created or received on behalf of, the CE or
  - if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- Authorize termination of the contract by the CE, if the CE determines that the BA has violated a material term of the contract unless such authorization is inconsistent with the statutory obligations of the CE or its BA.

Data Use Agreements. A Business Associate Contract is not required if the covered entity discloses only a limited data set to a business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate.

One more thing for a BA specifically to keep in mind:

A BA is not in compliance if the BA knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor’s obligation under the contract or other arrangement, unless the BA took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

BA Agreements Compliance Date:

BA Agreements must be in compliance with the new Omnibus requirements as of September 23, 2013 unless a compliant written contract was in place prior to January 25, 2013 and was not renewed between
March 26, 2013 and September 23, 2013, then that prior contract or other written arrangement is deemed compliant until September 22, 2014 or the date it is renewed or modified on or after September 23, 2013, whichever is earlier.

**Enforcement Activities Underway**

The HITECH Act mandates that the DHHS OCR conduct periodic audits of both CEs and BAs for compliance with HIPAA. Following on the heels of the 2012 “compliance” audits of CEs (OCR acknowledged to be looking for weaknesses and best practices, with no punishments handed out for non-compliance), the 2014 OCR HIPAA Audits are expected to be about enforcement and disciplinary action. OCR officials have indicated that BAs will be on the audit list this year along with their service providers.

Although individuals have long been able to file a complaint to the Secretary if they suspect a CE is not complying with the regulations, the Omnibus Rule added BAs to the list. OCR implemented a new on-line complaint form in the 4th quarter 2013, making it easier than ever for someone to report to the Secretary of DHHS suspected violations of their, or anyone else’s, HIPAA privacy rights. As shown in the chart below, the number of complaints reported to OCR has been steadily increasing since the HITECH Act was enacted in 2009. Leon Rodriguez, former Director of OCR, has suggested that reported complaints may hit 1,500/month with the help of the easily submitted form and the general public’s increased awareness of their rights. OCR has stopped providing complaint data but the last report in 2014 confirmed his suspicions.

There’s one more way that an organization can be in OCR’s headlights and that’s with a reportable breach. Breaches must be reported by CEs to the Secretary of HHS either within 60 days of discovery (if over 500 individuals) or annually. Rodriguez described these reports as his “inventory.”

BAs have their own notification requirements in the Breach Notification Rule, which includes notification to the CE within 60 days of discovery with details of the breach (who, what, where, how, why) which will be used to notify the Secretary, the affected individuals, and possibly the media. Care should be taken by every BA and their subcontractors to ensure that contractual reporting requirements or state breach
notification regulations are not more stringent than HIPAA (which is likely to be the case), at which point the most stringent notification requirements must be followed.

An understanding of the definition of a breach and the four factors that must be considered, at a minimum, in a breach risk assessment should be documented and a process for that assessment developed that can be applied consistently and documented appropriately in the event of an security incident or privacy violation.xxvi

**The Ramifications of Non-Compliance**

Penalties for non-compliance have increased with the enactment of the Omnibus Rule which details and implements significant changes called for in the 2009 HITECH Act.

For one, the Secretary no longer has discretion on whether to investigate a complaint if a preliminary review of the facts indicates a possible violation of “willful neglect”xxvii and, if so determined, the maximum penalty under the Civil Monetary Penalty (CMP) System must be assessed, if not corrected within 30 days of discovery.xxviii

As a reminder, CMPs that are collected under the HITECH Act are required to be funneled back into the HHS’ enforcement budget.xxix The HITECH Act strengthened the enforcement by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision.

The change in the CMP structure is detailed below:

<table>
<thead>
<tr>
<th>VIOLATION TYPE</th>
<th>MINIMUM PENALTY</th>
<th>MAXIMUM PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100/violation; annual max of $25,000/repeat violations</td>
<td>$50,000/violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$100/violation; annual max of $25,000/repeat violations</td>
<td>$50,000/violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000/violation; annual max of $250,000/repeat violations</td>
<td>$50,000/violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>$50,000/violation; annual max of $1,500,000</td>
<td>$50,000/violation; annual max of $1,500,000</td>
</tr>
</tbody>
</table>

The new penalty structure is as follows:

<table>
<thead>
<tr>
<th>VIOLATION TYPE</th>
<th>EACH VIOLATION</th>
<th>REPEAT VIOLATIONS/YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

7 HIPAA Primer Requirements for Business Associates
Other definitions provided in § 160.401. Definitions that are applicable here include:

- **Reasonable cause** means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.
- **Reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- **Willful neglect** means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

In determining the amount of any civil money penalty, the Secretary may consider as aggravating or mitigating factors, as appropriate, any of the following:

(a) The nature of the violation, in light of the purpose of the rule violated.
(b) The circumstances, including the consequences, of the violation, including but not limited to:
   (1) The time period during which the violation(s) occurred;
   (2) Whether the violation caused physical harm;
   (3) Whether the violation hindered or facilitated an individual's ability to obtain health care; and
   (4) Whether the violation resulted in financial harm.
(c) The degree of culpability of the covered entity, including but not limited to:
   (1) Whether the violation was intentional; and
   (2) Whether the violation was beyond the direct control of the covered entity.
(d) Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to:
   (1) Whether the current violation is the same or similar to prior violation(s);
   (2) Whether and to what extent the covered entity has attempted to correct previous violations;
   (3) How the covered entity has responded to technical assistance from the Secretary provided in the context of a compliance effort; and
   (4) How the covered entity has responded to prior complaints.
(e) The financial condition of the covered entity, including but not limited to:
   (1) Whether the covered entity had financial difficulties that affected its ability to comply;
   (2) Whether the imposition of a civil money penalty would
jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and
(3) The size of the covered entity.
(f) Such other matters as justice may require.

If you have not already done so, we recommend implementing the following steps immediately.

What do I do now?
If you have not already done so, we recommend implementing the following steps immediately. Thoroughly document each step to position your organization to demonstrate compliance.

1. Establish a HIPAA Compliance Officer and a HIPAA Oversight or Governance Team to determine and oversee the establishment of an appropriate compliance program.
2. Identify and document where all the PHI “lives” in your organization—paper, electronic, or oral—and its purpose.
3. Identify applicable HIPAA requirements based on the activities of your organization. [see Clearwater Compliance whitepaper for Security and Privacy Rule requirements for BAs]
4. Reduce the amount of PHI provided to your subcontractors to the minimum necessary for the functions provided.
5. Conduct rigorous Privacy, Security and Breach Notification compliance assessments to determine gaps or weaknesses in applicable HIPAA requirements. Document and act on a remediation plan to close any identified compliance gaps.
6. Implement or update comprehensive HIPAA Privacy, Security, and Breach Notification Policies & Procedures to address any gaps in requirements.
7. Train employees on new and/or updated policies and procedures immediately (and thereafter at least annually) and clearly define the disciplinary consequences to employees if they fail to adhere. Maintain accurate records of all training performed.
8. Identify and risk rate current subcontractors; establish or update a proactive program to update, as needed, BA agreements and a monitoring program to ensure reasonable safeguards are in place and privacy violations or security incidents are being promptly reported.
9. Know your state regulations and contractual requirements with your CEs re: incident and breach reporting.
Tools to Help BAs Comply

Whatever the state of your organization’s readiness for the enforcement of HIPAA Omnibus Rule, take advantage of resources available to ensure or strengthen compliance.

- Download a HIPAA Risk Analysis Buyer’s Guide Checklist™
- Participate in an intensive HIPAA Compliance BootCamp™
- Attend a Live HIPAA-HITECH Web Event this Month
- Download the Clearwater Business Associate Omnibus Checklist
- Download a Clearwater Compliance Whitepaper HIPAA Privacy Rule Requirements for Business Associates
- Download a Clearwater Compliance Whitepaper HIPAA Security Rule Requirements for Business Associates

For additional resources, visit www.clearwatercompliance.com
Endnotes

1 Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information means 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 in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

160.103 Definitions. Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.103 Definitions. Business Associate

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of a covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information.

(2) Business associate includes:

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) Employment records held by a covered entity in its role as employer.

§ 160.102 Applicability and § 160.103 Definitions

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

§ 160.103 Definitions. Business Associate

(3) Business associate includes:

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

§ 160.103 Definitions. Business Associate

(2) A covered entity may be a business associate of another covered entity.

§ 160.103 Definitions. Business Associate

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) Employment records held by a covered entity in its role as employer.

§ Other Situations in Which a Business Associate Contract is NOT Required.

from the Preamble to the OFR

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Section 13408 also provides that the data transmission organizations that the Act requires to be treated as business associates are those that require access to protected

HIPAA Primer Requirements for Business Associates
health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates. This is consistent with our prior interpretation of the definition of “business associate,” through which we have stated that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates. See http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html.*

* § 164.501 Definitions. Payment means:
(i) The activities undertaken by:
   (I) Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
   (II) A health care provider or health plan to obtain or provide reimbursement for the provision of health care;

* § 164.502 (e) Disclosures to business associates (1)(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with §164.504(e)(iii), that the subcontractor will appropriately safeguard the information.

* § 164.502 (e) Disclosures to business associates (1)(iii) ... A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

* § 164.504 (e)(1) Standard. Business associate contracts

* § 164.504 (e)(3) Other Arrangements (iv) ...