HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

# Compliance TODAY

April 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

## Why are so many DLA Piper employees certified in compliance?

*See page* 16

by Martha Ann Knutson, JD, CHC

# To be—or not to be—a business associate

» The HIPAA Omnibus rule created changes in relationships between covered entities (CEs) and their business associates (BAs).
» BAs are now directly liable for criminal and civil penalties under HIPAA.
» Subcontractors of BAs may also be liable for HIPAA violations.
» Carefully defining and training workforce members may limit both BA and CE liability.
» CEs and BAs have at least until September 23, 2013 to amend existing relationships.

***Martha Ann Knutson*** *(maknutson@MKnutsonLaw.com) practices law in California, Maryland, and the District of Columbia.*

Since the first publication of the HIPAA Privacy and Security rules, covered entities (CEs) and their contractors have spent countless hours in negotiations about whether or not the contractor was also a business associate (BA) and if so, what the CE and its BA needed to do as a result. Some BA relationships were easy to spot; some needed discussion, debate, and/or clarification from the agencies responsible for enforcing the rules. Those entities that were destined to become BAs to many others and those CEs destined to have many BAs both wanted the comfort and security of "their" form, so "form battles" were frequent and occasionally hard fought.

Knutson

On January 25, 2013 the federal Office for Civil Rights (OCR) published a long awaited final rule[1] implementing changes required by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. That rule will, once again, open up the debates on what it means to be—or not to be—a BA. For example, one particularly significant change it makes in the BA/CE landscape is the extension of direct liability for civil and criminal penalties to BAs, if they fail to maintain compliance with HIPAA and HITECH restrictions. Another is that an important liability limitation for CEs has been removed from the regulations. Putting it simply, BA agreements won't be going away, but the stakes relating to these relationships have changed considerably.

The "business associate" concept exists nowhere but in HIPAA compliance efforts. It has been a few years since the last round of debates over who is and who is not a business associate. This article is intended as a review of the most recent regulatory definition, a digest of the guidance issued by OCR since 2002 about who is and is not a BA, as well as an explanation for BAs and CEs alike on what this relationship means going forward.

## Who is definitely a business associate

In 2009 the HITECH Act simply adopted the definition of "business associate" from the then existing HIPAA regulations. The recently issued rule modified that definition slightly, so going forward, a BA is an individual or company that:

> on behalf of such covered entity…, 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*… or who *provides*,

other than in the capacity of a member of the workforce of such covered entity, *legal, actuarial, accounting, consulting, data aggregation…, management, administrative, accreditation, or financial services…* where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement[2] (emphasis added)

The BA definition also includes "persons" working for an "organized health care arrangement" (OHCA, defined in the rule as essentially a collaborative care arrangement, such as a hospital and its medical staff) made up of covered entities. "Person" is further defined as "a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private." However "persons" that are part of the covered entity's or a business associate's "workforce" are not business associates.

So the critical parts of the BA definition remain: (1) Work on behalf of a covered entity or OHCA that requires (2) access to, or use, disclosure, or maintenance of protected health information (PHI).

A BA still can be authorized under a BA agreement to do anything with the information that the covered entity may—but no more. A BA still may not use the PHI for its own purposes, or to serve other clients. It may use the information only for the function(s) it has contracted to perform for the covered entity, the BA's own "management and administration," and for complying with requirements of other laws.

**Past guidance from OCR**

In December 2002, OCR published a lengthy guidance document[3] which contained nine pages of FAQs relating to the business associate provisions of the rule. Those FAQs added a lot of clarity to the definition of those "persons" who were and were not to be considered BAs (see table 1).

**Table 1: Definitions of business associates**

| BAs | Not BAs |
|---|---|
| Accreditation agencies | A researcher (other restrictions apply), recipient of a limited data set, or user of de-identified information |
| A covered entity hired by another covered entity to do something other than treatment, unless a they are a workforce member (e.g., a contracted medical director, trainer) | Those to whom disclosures are made for purposes of treatment, including placement and discharge activities, laboratories, reference labs, pharmacies, contact lens suppliers |
| Shredding companies where the work is done off site | Onsite shredding (if defined as part of the CE workforce) |
| A person involved in de-identifying data/creating a limited data set | Those whose work might involve inadvertent/incidental exposure to information (e.g., janitors, plumbers, electricians, photocopy repairmen) |
| Software vendor who hosts software containing PHI offsite OR whose employees must access PHI while remotely troubleshooting issues in software hosted by the covered entity | Software vendor who does not have access to PHI or whose employees only work on the system onsite at the covered entity's premises (i.e., workforce) |
| Transcriptionists, unless they are part of the defined workforce | Other members of an Organized Health Care Arrangement (OHCA) (e.g., physicians with medical staff privileges at a hospital or surgery center, a health plan and the HMO it contracts with) |
| | "Mere conduits" of information (e.g., USPS, UPS, delivery truck employees and their management, telephone companies, Internet Service Providers) |
| | Providers being paid by a health plan/government program for treating members of the plan/program |
| | Banks performing debit or credit transactions from patients to covered entities |
| | "Persons" that a covered entity is required to provide information to so as to "fulfill a legal duty" |

What the FAQs also made clear is that there are at least three potential arguments against BA status for a particular "person":

- their inclusion in the covered entity's workforce (the workforce exception),

- their exposure to PHI is "incidental or inadvertent" (the janitor or workman exception), or
- they are a "mere conduit" of the information taking it from one "place" to another (the FedEx exception).

In the latest version of the rule, OCR added the term "maintain" to the BA definition, apparently in response to arguments from record storage companies and "cloud" data service providers that the "mere conduit" rationale applied to them as well. Although "transient storage" of PHI will not create a BA relationship, apparently "less transient" will, going forward.

## The opportunity to object (or agree) exception

OCR has also posted FAQs about the HIPAA Privacy and Security rules, from time to time, on its website. One of these, first published in April 2004, clarified that if a patient had the opportunity to "agree or object" prior to the disclosure of information, the "person" to whom the disclosure was made is not a business associate. The specific situation analyzed was the use of a telecommunications relay service to communicate with a patient who is deaf or hard of hearing. Either the patient or the provider initiates the call through the relay service, which simply acts as a "communications assistant" according to OCR. In either case the patient, in theory, has the opportunity to "agree or object" to the "assistant's" exposure to their PHI. The FAQ also states that permission could also be obtained ahead of the call from the patient, for example, during a prior office visit.[4]

The same "opportunity to object" rationale might be applied to other circumstances where the exposure to the patient's PHI is apparent or the patient is given a specific "opportunity to object" before it occurs. For example, in-person interpreters or transcriptionists and the companies they work for may well not be BAs. The same rationale would apply to those providing these services by real-time video link.

Further, there are websites that provide information about a certain disease state, therapies, etc. To direct a viewer to useful information, the site may request that he/she pick from lists of symptoms, or the site simply records the "clicks" he/she makes and provides access to information based on an algorithm. What if the site also offers referrals to physicians (who contract with the site to accept them) and transfers personally identifiable information to the chosen referral source? Is the website operator a BA to those physicians, or just a "communication assistant," if the site's role is simply transferring information between patient and potential provider at the patient's request via a "click"?[5]

## New business associates

The January 2013 final rule incorporated several additional entities into the definition of a business associate that were required by the HITECH Act as well as one proposed by OCR.

Specifically, OCR expanded the rule to include "patient safety organizations"(PSOs), as long as they are not components of the covered entity (the "workforce" exception continued). OCR acknowledged that these organizations arguably already fit within the original definition, but proposed the clarification to more closely align HIPAA and a different federal rule relating to patient safety.[6]

**Those who facilitate data transmissions**

Health information exchange organizations (HIOS), their cousins—the regional HIOS (RHIOS), e-prescribing gateways, personal health record vendors, and other "persons" who facilitate data transmissions were all added to the BA category by the HITECH Act.[7] Personal health record vendors were added to the extent that their product is offered as an extension or part of a CE's electronic medical record.

Both the HITECH Act and OCR continued the "mere conduit" rule of interpretation by distinguishing between data transmission organizations that routinely require access to the data they transmit and those that don't, indicating in the commentary that the latter are not considered business associates. What is a "data transmission organization" and how often is "routinely"? That's "fact specific" and is decided on a case-by-case basis.

**BAs of BAs (a.k.a. subcontractors)**

Under the final rule, subcontractors of a BA are also explicitly included in the definition of business associate. The commentary to the proposed rule made it clear that this extension to downstream entities is an agency creation, particularly the statement that this extension of liability is "consistent with Congress' intent."[8] Significantly, OCR stated that the first tier BA will not have to enter into a formal contract with the downstream entity, but the first tier BA must still obtain written "satisfactory assurances" that its contractor will comply.

This extension of direct responsibility for HIPAA compliance to downstream entities is one of the most significant portions of the rule, since many "persons" who have not even signed a business associate agreement in the past may now find themselves directly liable for breaches of a set of regulations that they have only limited knowledge of.

**Who's in the "workforce"?**

One caveat to characterizing an entity as a BA is when a CE is prepared to accept the "person" or its people as part of the CE's "workforce." The workforce concept was first introduced to extend coverage of the Privacy Rule's obligations to "volunteers, trainees, and other persons.… [w]hether or not they are paid by the covered entity."[9] Employees are part of the workforce,

but not all workforce members are employees. Subcontractors of BAs could also be BA workforce members, going forward.

Another factor that distinguishes a workforce member from a BA is not what they do or who pays them to do it, but where the work is to be performed. As OCR put it in 2002:

> If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed *under the direct control* of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.[10] (emphasis added)

What, besides location, is necessary to establish "direct control"? Neither the original rules, the HITECH final rule, or interim publications from OCR provide any guidance.

So if a CE (and now, a BA with reference to its subcontractors) is willing to characterize a particular set of workers as part of its workforce, it can effectively relieve their potential BA employers from the direct liability imposed by the HITECH rule. With this decision, the CE or BA also exchanges its burden of obtaining "satisfactory assurances" from the contractor for a duty to train the "workforce" members in its policies and procedures.

Some counsel may object that recognizing a "workforce" characterization unnecessarily admits agency liability for any errors or omissions of the individuals involved. But OCR clearly refuses to draw bright lines for potential liability based on the characterization of whether or not an individual is a business associate or a workforce member. Either may be an "agent" for purposes of imposing liability under the federal law of agency, according to OCR, based on the facts and circumstances of the particular case.[11] The more significant argument is whether or not a given individual was acting within the scope of his or her agency. Rarely—if ever—will a CE or a BA give anyone authority to violate the requirements of the HIPAA Privacy and Security Rules.

## Shifting incentives

The final rule also takes away a significant incentive of CEs to characterize their contractors as BAs rather than workforce. Under earlier versions of 45 CFR 160.402, "Basis for Civil Monetary Penalty," if an "agent" was a characterized as a BA and a CE had an appropriate agreement in place, the CE was exempt from civil monetary penalty (CMP) liability for its BA's missteps, unless it knew of a "pattern of activity" on the part of the BA that would result in violations of the privacy and security rules and failed to respond to them. That exception to principal liability has been removed by the final HITECH rule.

So going forward, both CEs and BAs will be responsible for the authorized missteps of their "agents." It is worth taking a look at the facts and circumstances of the work performed, including its location, rather than starting from a presumptive characterization of BA for all contractors, volunteers, or trainees. Especially for those working on the CE's or BA's premises alongside its volunteers and employees, the best compliance approach may be to ensure that these individuals are adequately trained, rather than simply relying on promises to that effect in a BA agreement and looking the other way if they violate policies and procedures of the CE or BA. Training may also minimize liability in the event of a

"rogue" agent that consciously violates policies and procedures, since it can be used to establish that he/she knew they were not authorized to act in that way (e.g., accessing the PHI of a spouse during a divorce proceeding) and the BA or CE took reasonable steps to prevent the rogue's intentional rule violation.

### BA or not a BA—Why it matters to the BA

The HITECH Act and the final rule make several changes to the responsibilities and potential liabilities of BAs. As mentioned above, BAs are now directly liable for HIPAA criminal and civil liabilities "in the same manner" as CEs. BAs may also be liable for their subcontractor "agents." These changes alone will surely lead to many demands that CEs reassume this potential liability through contractual indemnity or limitation of liability provisions. CEs, of course, will have every reason to resist such demands, not only because they suggest a rather laissez faire attitude about compliance from the beginning of the relationship, but because they would create an unlimited and likely uninsured potential liability.

OCR was asked by at least one commentator to amend the rule to prohibit such shifts of liability provisions in BA agreements and wisely chose to leave this debate to the parties involved in each contract. BAs should take some comfort, however, from the removal of the requirement that CEs notify the Secretary of Health and Human Services when they determine that a BA's actions are violating the rule but it is not "feasible" to terminate their agreement with the BA.

### Liable for what exactly?

Becoming directly liable for liability under the HIPAA rules does not mean that a BA assumes all the HIPAA responsibilities of a CE, a point well illustrated by an example in the commentary to the proposed rule. Assume a CE

hires a BA to deliver the CE's Notice of Privacy Practices (NPP). When the BA fails to do so, the CE is liable under the Privacy Rule for the failure of its chosen agent, but not the BA—because the BA didn't have a duty under the Privacy Rule to deliver a NPP. (The BA will, of course, probably be liable for breach of its contract with the CE.)

Further, BAs will bear direct responsibility (and potential liability) for:

- limiting uses and disclosures of PHI to those permitted under the BA agreement;
- designating personnel responsible for security compliance if they have e-PHI;
- performing a risk analysis (if they have e-PHI);
- establishing policies that incorporate technical and administrative safeguards for the PHI–in whatever format they have been entrusted with;
- investing in hardware and software to prevent and monitor internal and external breaches of E-PHI;
- notifying the CE of breaches of unsecured PHI "without unreasonable delay";
- executing written "assurances" with subcontractors that pass on these same responsibilities;
- providing information in response to an individual's request for a copy of his/her PHI (to the individual or the CE as specified in the BA Agreement); and
- keeping records and cooperating with OCR investigations and compliance reviews.

In fact, in its burden analysis for the rule, OCR stated an assumption that existing BAs who are doing what their BA agreement says they will do should have little additional compliance cost or effort as a result of these changes. OCR's goal is to "incentivize" those who are not following existing agreements more strongly.

**What's the deadline?**

The compliance date for meeting the obligations under the final rule is September 23, 2013, with one notable exception. Recognizing that some amendments to BA agreements may be necessary, as it did with the original Privacy Rule, OCR has provided for a transition period beyond the compliance date to get those revised agreements in place. Although OCR estimated that amendments to existing BA agreements should take only an hour of legal time per relationship, BA and subcontractor relationships that are (1) in existence on the publication date (January 25, 2013); and (2) are not renewed or modified between the "effective" and the "compliance" dates are grandfathered for up to one year (September 23, 2014).[12] "Evergreen" contracts (i.e., those containing automatic renewals) are eligible for the extended transition period. Oral agreements are not.

## More to come

OCR has a statutory duty under the HITECH Act to provide education to BAs about their new liabilities and responsibilities. Those efforts will undoubtedly bring more clarification and detail as to the OCR's expectations. Until then, BAs and their CEs will undoubtedly reassess their existing relationships and the "form battles" will be underway again.

1. 78 FR 5566 – 5702 (January 25, 2013)
2. 45 C.F.R §160.103 (emphasis added)
3. Office for Civil Rights: "Standards for Privacy of Individually Identifiable Information" (Privacy Guidance) December 3, 2002. Some of the FAQs from this document have since been duplicated on the OCR website, but this document is no longer available in its entirety there. Contact the author by email for a copy in electronic format.
4. See also 45 CFR § 164.510
5. See also OIG Advisory Opinion No. 02-12 at 10 (2002) - the "clicking" by a website viewer helps "ensure the voluntariness of a subsequent transaction."
6. The Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b–21, et seq.
7. Section 13408, 42 U.S.C. 17938 (February 17, 2009)
8. 75 FR 40873 (July 14, 2010)
9. 45 CFR 160.103
10. Privacy Guidance at 48.
11. See, e.g., 70 FR 20224, 20232-33 (2005); 71 FR 8390, 8402-03 (2006); § 160.402 and accompanying commentary in the 2013 rulemaking
12. §164.532(f)