CHRISTIANSEN IT LAW

WWW.CHRISTIANSENLAW.NET

Information Technology Law | Privacy / Security / Compliance | Contracting, Risk Management & Due Diligence

The HITECH Business Associates Rule Tool:

Finding Your Place and Planning Compliance

In the New Ecology of Healthcare Privacy and Security

John R. Christiansen
Christiansen IT Law
2212 Queen Anne Avenue N. #333
Seattle, WA 98109
Phone: 206.301.9412
Email: john@christiansenlaw.net
www.christiansenlaw.net

Contents

Section 1: Introduction

This HITECH Business Associates Rule Tool is a guide to some of the key implications of the Business Associate provisions of the HITECH regulations published in January 2013, which amended the HIPAA Privacy and Security Rules published several years before.

This is a somewhat complex area, and the regulations are by no means intuitive. This Tool is intended to cut through some of the complexity and help users think through some of the issues more easily. It is not a law review article or especially intended for lawyers, though some lawyers may find it helpful. It does assume some familiarity with HIPAA, but deep knowledge shouldn't be required.

This Tool was originally published as a series of linked blog posts, which are still available at the Christiansen IT Law blog.

This Tool and the information it provides are not intended to be legal advice. The determination whether a given individual or organization is or is not a Business Associate, and what it might mean, has to be made on an analysis of the specific facts applicable to the individual or organization. If you want legal advice you are certainly welcome to contact me about setting up an engagement, but you are welcome to use the Tool to educate yourself without doing so. Just keep in mind that any decisions you make using it are yours alone and are not based on my legal advice, and any errors you make are your own responsibility.

While I have done my best to make sure the information in this Tool is accurate, I can't guarantee it. I also have tried to come up with the most reasonable and informed interpretations of the rules I can, but others, particularly regulatory authorities, may disagree with some of them. I do expect to update this Tool if it appears people are finding it useful, but can't guarantee I will do so.

I would appreciate informed comments and questions and will respond to them as I can. I moderate the comments but please keep in mind that questions and comments which are published will be visible to anyone else who uses the Tool. You should therefore not include information or details which might be sensitive in some way. If you would like to comment or ask questions confidentially you can email me.

Section 2: Background and Concepts.

On January 17 the U.S. Department of Health and Human Services (DHHS) published the unofficial version of the HITECH Megarule, or to call it by its proper name, "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." This is the biggest expansion and revision of HIPAA and its rules dealing with Protected Health Information (PHI) to date.

The Megarule is scheduled for official publication in the Federal Register on January 25, with an effective date of March 26 and a "Compliance Date" of September 23, 2013. The Compliance Date is the date on which Covered Entities and Business Associates will be required to be in compliance with the new rules, with the exception of new Business Associate Contract requirements for those which have existing Business Associate Contracts which are "deemed compliant." This will be reviewed in Section 7.

While the Megarule covers a number of subjects (as its name indicates), its most significant and widely applicable change to HIPAA is a greatly expanded regulatory authority over organizations which work with Protected Health Information ("PHI") directly or indirectly on behalf of Covered Entities – HIPAA's Business Associates, but under a greatly expanded definition of that term.

Business Associates and Subcontractors under HIPAA before HITECH.

The reason for this change in Business Associate status is that HITECH changed HIPAA's somewhat peculiar jurisdictional structure. HIPAA itself was limited in application to health care providers, health plans and health care clearinghouses – HIPAA's Covered Entities - because HIPAA was really only secondarily about privacy and security. Since HIPAA didn't reach other kinds of entities which Covered Entities needed to use for legitimate purposes, which needed to be able to use and disclose PHI for those purposes, the HIPAA regulations created the category of "Business Associate."

Since HIPAA couldn't reach Business Associates directly, it reached them indirectly by requiring Covered Entities to have Business Associate Contracts with Business Associates before allowing their Business Associates to create, receive or transmit PHI for any activity, function or service they perform for or on behalf of the Covered Entity. Business Associate Contracts must meet specified regulatory requirements which pass along key Covered Entity obligations to their Business Associates. Covered Entities were required to terminate their Business Associate Contracts for uncured contract violations, and could be penalized for failing to have Business Associate Contracts when required, or failing to take action if they found out their Business Associate was in violation.

Of course, many Business Associates in their own turn need or want to use still other organizations to provide services or perform activities involving PHI, so the Business Associate can fulfill its own obligations to a Covered Entity, as shown in the following examples:

- A health information organization ("HIO") which manages health information exchange ("HIE") services for a community of health care providers might contract with a cloud services provider to host its record locator service. Since HIE is an activity which

involves PHI the health care providers are Covered Entities, and the HIO is a Business Associate.

- A security consulting firm which is providing breach response services to a health insurance carrier might contract with an electronic evidence processing firm to assist in forensics and retention of digital evidence for possible use in litigation. If the breach involves PHI the health insurance carrier is a Covered Entity, and the security consulting firm is a Business Associate.

Under HIPAA before HITECH, in these examples the cloud services provider and the electronic evidence processing firm are both "Subcontractors." Of course, Subcontractors were also not subject to HIPAA jurisdiction, a situation the HIPAA regulations managed by requiring Business Associate Contracts to include a provision allowing the Business Associate to use Subcontractors only if the Business Associate in turn had a contract which passed along some (but not all) of the Business Associate Contract obligations.

Neither Business Associates nor Subcontractors were subject to regulatory investigation or penalties under HIPAA before HITECH, and for many organizations this has led to some confused or lax practices, especially among Subcontractors – many of which may not even realize they have significant obligations. HITECH has now changed all this.

Business Associates and Subcontractors under HITECH.

HITECH stands for the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which became law on February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009 ("ARRA").

As with HIPAA, the primary purpose of HITECH wasn't really to be a privacy and security law. Rather, the central concern in HITECH was providing incentives for and facilitating the implementation of electronic health records ("EHRs"). As with HIPAA, however, the privacy and security aspects of HITECH are likely to wind up being the most significant for many organizations.

HITECH created new privacy requirements for both Covered Entities and Business Associates, including restrictions on disclosures by providers to health plans, changes to the minimum necessary standard, accounting requirements for disclosures made through electronic health records, and restrictions on marketing and fundraising. HITECH also established mandatory breach notification requirements and enhanced civil and criminal penalties. The most dramatic change, however, was the extension of jurisdiction beyond Covered Entities to Business Associates.

Not all HIPAA and HITECH requirements which apply to Covered Entities apply to Business Associates, but the Security Rule, breach notification requirements and a number of privacy requirements do. There are now teeth in these requirements, too, as Business Associates are now subject to regulatory investigations and to civil – and criminal – penalties for failure to comply. Since HITECH did not get rid of the Business Associate Contract requirement they may in fact face "double jeopardy" for compliance failures, and be exposed not only to regulatory but contractual penalties.

The Megarule also took the logic of HITECH a perhaps unexpected step further, and amended the definition of Business Associate to include Subcontractors – and required Subcontractors-as-Business Associates to in turn have Business Associate Contracts with their Subcontractors; who in turn, of course, are Business Associates required to have Business Associate Contracts with their Subcontractors, and so on down a contractual chain as far as activities involving PHI on behalf of a Covered Entity are subcontracted.

A Business Associate under the Megarule is therefore any organization which "creates, receives, maintains, or transmits" PHI for purposes of a service or activity performed for or on behalf of, or provided to a Covered Entity, directly or indirectly. The scope of the uses and disclosures of PHI the Business Associate may make is established in its Business Associate Contract, and a "downstream" Business Associate Contract must be at least as restrictive, and may be more restrictive, than the "upstream" contract from which it depends.

Of course, Business Associates have their own legitimate business or operational needs to have third parties perform services which are for the use or benefit of the Business Associate only, but which involve access to, use or disclosure of PHI the Business Associate has under a Business Associate Contract. For example, a third party administrator ("TPA") which is the Business Associate of a Taft-Hartley health benefits plan might need to retain a law firm to help it determine its potential exposure in a security breach involving plan PHI.

The HIPAA rules before HITECH recognized this, and provided that a Business Associate Contract could permit the Business Associate to disclose PHI to a third party for the Business Associate's own purposes if it has assurances the third party will keep the PHI confidential and report any breach of confidentiality to the Business Associate. This provision was retained, and third parties providing services to Business Associates for the Business Associates' own purposes are not considered Subcontractors (i.e., are not themselves Business Associates). There is no regulatory definition for such third parties, who will be called "Business Associate Services Providers" for convenience.

Business Associates under the HITECH Megarule: A Chain of Trust with Teeth[1]

The Business Associate provisions of the Megarule[2] establish some of the most dramatic changes to the HIPAA regulations since initially published. The HIPAA jurisdictional limitations which narrowed the application of the regulations to covered entities[3] were removed by the HITECH Act. Now the regulations apply not only to covered entities, but to any other entity which works

[1] Originally published in American Bar Association Health Law Section, ***Health eSource HIPAA Megarule Special Edition Part 1*** (January 29, 2013), available at http://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_esourcejanuary2013volume9hipaamegarulespecialeditionp.html.

[2] U.S. 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, 78 Fed. Reg. 5566 (January 25, 2013).

[3] See definition of "covered entity" at 45 C.F.R. § 160.103. This definition was not amended by the Megarule.

with protected health information ("PHI") for any purpose of a covered entity, directly or indirectly. All such entities are now business associates, whether they know it or not.[4]

The Megarule also extended Security Rule and select Privacy Rule obligations directly to business associates,[5] while retaining the requirement that covered entities establish and maintain business associate contracts[6] with their business associates and extending it to require that business associates in turn have business associate contracts with any subcontractor to which they delegate any service, function or activity involving PHI on behalf of the covered entity.

Business associate status attaches upon creation or receipt of PHI for a regulated function, activity or service, not by entry into a business associate contract or other agreement.[7] Because this status attaches automatically, the Megarule creates an automatic "chain of trust" which follows the PHI from business associate to business associate. Each party in the chain is required by regulation and by contract to protect the PHI and administer it consistently with the obligations of the covered entity at the top of the chain:

Thus, under the final rule, covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far "down the chain" the information flows. This ensures that individuals' health information remains protected by all parties that create, receive, maintain, or transmit the information in order for a covered entity to perform its health care functions.[8]

---

[4] The rules distinguish between arrangements between business associate contracts involving non-governmental entities; "other arrangements" which are the equivalent between governmental entities; and plan document terms, which apply between group health plans and their sponsors. While there are some differences and different implications among these, most of the issues discussed apply to all three types of arrangement and for convenience this article will only address the first category.

[5] See 45 C.F.R. § 160.103 for the definition of "business associate." This definition was amended by the Megarule. The Security Breach Notification Rule was promulgated before the Megarule but under the HITECH Act, which gave jurisdiction for its application to business associates, and therefore already applies to them.

[6] "Business associate contract" is not defined in the regulations, but is the term used in 45 C.F.R. §§ 164.314 and 164.504(e) for the form of the "reasonable assurances" a covered entity is required to obtain from its business associates. Confusingly, the HITECH Act itself refers to business associate contracts as "business associate agreements." See §§ 13401(a) and 13404(a) of Title XIII of the American Recovery and Reinvestment Act, Pub.L. 111-5 (February 17, 2009) (H.R. 1), the Health Information Technology for Economic and Clinical Health Act ("HITECH"). This appears to be a distinction without a difference, and this article will use the regulatory term for convenience.

[7] Megarule at 5598.

[8] Megarule at 5574. Compare the "chain of trust partner agreement" proposed in the draft Security Rule:

> Contract entered into by two business partners in which it is agreed to exchange data . . . where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originating party to the ultimate recipient[.]

Each party in this chain will be subject to often redundant regulatory and business associate contractual obligations, and therefore may be subject to both civil monetary penalties and contractual remedies for violations. This is truly a "chain of trust with teeth."

The extension of business associate status and obligations as published in the Megarule therefore has crucial implications for two categories of entity:

- Current business associates are now directly exposed to regulatory penalties, which may mean they will want to or should re-assess their legal risks and compliance strategies. They will also have to review and revise their subcontracting strategies. While ideally existing business associates should have been staying abreast of the developing law, the reality is that many probably have not, and will need to be advised and supported in understanding their new obligations and exposures.
- Entities which act as subcontractors to business associates will also need to review their legal risks, compliance and contracting strategies, and it is even less likely that this kind of party will be aware of the new developments and their implications. They are therefore even more likely to need good advice and support.

Making this kind of chain work properly will take some cooperation among its "links," so it is worth analyzing the concept further.

Explaining the Chain

Clear discussion of business associate chain of trust issues probably requires some new vocabulary, as use of the terminology within the Megarule can lead to convoluted and confusing phrasing.

A business associate chain of trust starts at the top with a covered entity. The covered entity is required to have a business associate contract with any entity which it allows to create, receive, maintain or transmit PHI for purpose of providing services or performing functions or activities to or for the covered entity, and that entity is a business associate. This, aside from the addition of the term "maintain" to the definition, is essentially the established concept and definition of a business associate.[9]

The Megarule then provides that this first business associate may start a chain of subsequent business associates. It does so by creating a new definition of "subcontractor" as a "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such a business associate", and expanding the definition of business associate to include a "subcontractor that creates, receives, maintains, or transmits [PHI] on behalf of the business associate."[10] This means that subcontractors, which previously

---

U.S. Department of Health and Human Services, Security and Electronic Signature Standards; Proposed Rule, 63 Fed.Reg. 43242 (August 12, 1998) at 43272.

[9] See 45 C.F.R. § 160.103, definition of "business associate" as amended by the Megarule.

[10] 45 C.F.R. § 160.103, as amended by the Megarule.

were only regulated second-hand by subcontractor provisions requiring business associates in general terms to pass along protection requirements,[11] are now full-fledged business associates – as are their subcontractors in turn. Covered entities are not required to have direct business associate contracts with subcontractors,[12] so obligations flow down the chain of arrangements and contracts.

There is considerable potential for confusion about different business associates and subcontractors in a chain of any length, and analyses may be simpler with some clarifying terminology. One set of useful terms would be to refer to "upstream" and "downstream" business associate contracts,[13] with the upstream business associate contract establishing a business associate's authority with respect to PHI, and the downstream business associate contract establishing the authority of an entity to which a business associate has delegated an activity, function or service involving PHI.

Another useful term is "tier," referring to the business associate's level in the chain of trust:[14] The business associate at the top of the chain, which has a direct business associate contract with a covered entity, is a first tier business associate; the entity with a direct business associate contract with a first tier business associate is a second tier business associate; and so on. Business associates below the first tier would then be lower tier business associates.

An example might help demonstrate this approach. Consider a health information organization ("HIO") which manages health information exchange ("HIE") services for a community of healthcare providers. The HIO might contract with a data hosting service to maintain its record locator service. Since HIE is an activity which involves PHI, the healthcare providers are covered entities, and the HIO is a first tier business associate.[15] The data hosting service in turn would be the "downstream" business associate of the HIO, and a second tier business associate.

While each business associate in a chain will have the same set of regulatory compliance obligations, they may not have the same authority with respect to PHI. Business associates are permitted to use or disclose PHI only as provided in their business associate contract or as required by law.[16] A business associate cannot pass on greater authority with respect to PHI than it has, so its downstream business associate contracts must provide PHI use and disclosure

[11] See 45 C.F.R. §§ 164.314(a)(2)(i)(B), 164.504(e(2)(ii)(D), prior to Megarule amendment.

[12] See 45 C.F.R. §§ 164.308(b)(1), .502(e)(1), as amended by the Megarule.

[13] This term is not included in the Megarule, but is suggested as a way of describing relationships in a business associate chain of trust more simply.

[14] This term is not included in the Megarule and is suggested as a simpler way of describing business associate chain of trust relationships.

[15] Expressly as well as implicitly in the Megarule expansion of the definition of "business associate." See 45 C.F.R. § 160.103 as amended by the Megarule.

[16] See 45 C.F.R. § 164.504(e)(2)(i).

limitations at least as stringent as, and if appropriate more stringent than, its own upstream business associate contract provides.[17]

Likewise, if obligations of the covered entity are being delegated down the chain, the business associate contracts must require any downstream business associate to which they are delegated to comply with the requirements which would apply to the covered entity's performance of that obligation.[18] For example, an electronic health records ("EHR") vendor might agree to be the access point for individuals wanting copies of their medical records, in which case the vendor as a business associate would have to comply with an upstream hospital covered entity's obligation to provide it in electronic format upon request, under the time limits which would apply to the Covered Entity.[19]

Finally, the business associate contract requirements still allow the contract to include a provision which permits a first tier or downstream business associate to disclose PHI for the business associate's "proper management and administration" or to "carry out its legal responsibilities," if the business associate obtains "reasonable assurances that the PHI will be "held confidentially" and "used or further disclosed only as required by law or for the purposes for which it was disclosed," and that the person to which it was disclosed will notify the business associate of any breach of confidentiality."[20] This provision applies only where the purpose of the disclosure is for purposes of the business associate and not for purposes of the covered entity at the top of the chain.[21]

For example, in the case of the business associate HIO, the downstream data storage business associate might experience a security incident and retain a computer forensics firm to advise it about the nature and scope of the breach. Forensics would require access to PHI to be effective, but because this would be a service specifically for the business associate the forensics firm would not become a business associate. A useful way to refer to this kind of relationship might be to call the forensics firm, or any entity in a comparable relationship, a business associate services provider.[22]

---

[17] See 45 C.F.R. § 164.504(e)(2)(ii)(H), as amended by the Megarule.

[18] See 45 C.F.R. § 164.524.

[19] See 45 C.F.R. § 164.504(e)(2)(i).

[20] See Megarule at 5574: "We also provide the following in response to specific comments. Disclosures by a business associate pursuant to § 164.504(e)(4) and its business associate contract for its own management and administration or legal responsibilities do not create a business associate relationship with the recipient of the [PHI] because such disclosures are made outside of the entity's role as a business associate."

[21] This term is not included in the Megarule and is suggested as a simpler way of describing business associate chain of trust relationships. Referring to such a party as a "business associate subcontractor" would risk confusion with subcontractors which are business associates, and a term such as "business associate subcontractor which does not perform functions, activities or services related to a covered entity" seems cumbersome and confusing.

[22] Megarule at 5601.

The fact that a provision allowing a business associate to disclose PHI to a business associate services provider is an optional element of a business associate contract has the potential to cause significant problems for downstream business associates. Since a business associate contract can only pass on authority with respect to PHI which is equal to or less than the authority provided in an upstream contract, a failure to include such a provision in a business associate contract at one tier would preclude it for any lower tier.

This could have serious consequences, for example, for the data storage business associate experiencing a breach, which would not have the authority to retain a computer forensics firm. This is clearly not a useful outcome either for the business associate or any party up the chain, so hopefully parties negotiating business associate contracts will recognize and avoid this kind of problem.

Conclusion

The revised and expanded business associate rules, concepts, and agency interpretations as discussed in the Megarule clearly have many potential implications beyond the scope of this article. Business associate contracts in particular will need reconsideration and perhaps new variations will need to be developed. Some of this work is already under way by the ABA Health Law Section, including a business associate contract template with commentary, and participation and assistance in this and related projects is welcome.

Other operational and legal implications will only become apparent as various parties try to figure out and negotiate their relationships under the revised rules, and as new business, operational and contracting arrangements are developed, perhaps especially for HIE and outsourced information technology services. Helping clients identify and resolve these issues promises to be an interesting process for some time to come.

Section 3: How to Tell If You're a Business Associate.

1. In order to determine whether you are a Business Associate, ideally before agreeing to or accepting any arrangement in which you will create, receive, maintain or transmit PHI, you should determine:
   a. Whether the party for or from which you will do so is a Covered Entity or a Business Associate,
   b. If the party is a Business Associate,
      (i) whether the purposes for which you will do so is a function, activity or service the Business Associate has agreed to provide or perform for or on behalf of a Covered Entity or another Business Associate, or
      (ii) Whether it is a function, activity or service for purposes of the Business Associate.
2. A Covered Entity is defined as any person (corporate entity or individual) which is:
   a. A Health Care Provider, including hospital, physician, clinic, laboratory, or any other provider of health care or medical services, which is paid for its services by electronic claims transactions;
   b. A Health Plan, including a health insurance carrier, employee group health benefits plan, government health plan, or any of a number of other health care payors; or
   c. A Health Care Clearinghouse, a health claims transactions processor.
3. A Business Associate is defined as any person (corporate entity or individual), including a Covered Entity, which:
   a. Creates, receives, maintains, or transmits PHI,
   b. In order to provide or perform a function or activity on behalf of a Covered Entity including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, benefit management, practice management, repricing, or services to a Covered Entity including but not limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial, health information exchange ("HIE") or personal health record ("PHR") services,
   c. Including not only a person which is providing or performing the function, activity or service directly to or for a Covered Entity ("First Tier Business Associate"), but also persons to which a First Tier Business Associate subcontracts or delegates some or all of the function, activity or service ("Second" or "Lower Tier Business Associate"), and so on downstream as far as functions, activities or services are subcontracted or delegated to other persons ("Lower Tier Business Associates").
   d. Business Associates do not, however, include:
      (i) Individual members of the Covered Entity's Workforce,

(ii) Covered Entities performing such functions or activities or providing such services to other Covered Entities, when they are all part of an Organized Health Care Arrangement.

(iii) Health care providers receiving PHI for purposes of treating an individual.

4. Business Associate status is "definitional," which means that a person becomes a Business Associate whenever conditions exist which meet the definition of Business Associate. A person can therefore become a Business Associate without knowing or wanting to become one, and without entering into a Business Associate Contract.

5. A Second or other Lower Tier Business Associate must be distinguished from a Business Associate Services Provider. Part of the definition of Business Associate is that it is acting for or on behalf of a Covered Entity, directly or indirectly, when dealing with PHI. A Business Associate Services Provider, on the other hand, is acting for or on behalf of a Business Associate, and a Business Associate Services Provider is not a Business Associate.

Section 4: Compliance as a Business Associate

1. Business Associates are directly responsible under the regulations for:

a. Implementing Business Associate Contracts with any downstream Business Associates;

b. Compliance with the Security Rule;

c. Using and disclosing PHI only as permitted by their Business Associate Contract;

d. Compliance with the Minimum Necessary rule;

e. Notifying their upstream Business Associate or Covered Entity (as applicable) in case of a security breach;

f. Providing access to a copy of the electronic PHI in their possession to either the Covered Entity, the individual, or the individual's designee, as specified in their Business Associate Contract;

g. Providing access to their records, including PHI, to DHHS for purposes of investigation of the Business Associate's compliance with its regulatory obligations; and

h. Providing the information needed for an accounting of disclosures.

(i) Compliance with these regulatory requirements will be mandatory as of September 23, 2013.

2. Business Associates will be responsible under their Business Associate Contracts for:

a. Implementing Business Associate Contracts with any downstream Business Associates;

b. Compliance with the Security Rule;

c. Reporting security incidents and breaches to their upstream Business Associate or Covered Entity, as applicable;

d. Using and disclosing PHI only as permitted by their Business Associate Contract;

e. Providing access to a copy of the PHI in their possession to either the Covered Entity, the individual, or the individual's designee, as provided in the Business Associate Contract;

f. Amending the PHI in their possession in accordance with the Business Associate Contract;

g. Providing access to their records, including PHI, to DHHS for purposes of investigation of the upstream Business Associate's or Covered Entity's compliance with its regulatory obligations (as applicable; and

h. Providing the information needed for an accounting of disclosures.

(i) These Business Associate Contracts overlap and are in many cases redundant to Business Associate direct regulatory obligations, but not entirely. Business Associate Contract provisions should ***not*** be inconsistent with the regulatory provisions they overlap.

(ii) First Tier Business Associates should already be subject to Business Associate Contracts which meet pre-HITECH HIPAA requirements. Such Business Associate

Contracts must be amended to be HITECH-compliant as provided in Determining the HITECH-Compliant Business Associate Contract Date.

3. Lower Tier Business Associates will be required to be subject to HITECH-Compliant Business Associate Contracts as of September 13, 2013.

Section 5: Penalties for Business Associate Noncompliance

OCR may impose civil monetary penalties on both CEs and BAs for violations of any of the requirements of the Privacy or Security Rules.

Where more than one CE or BA is responsible for a violation each may be subject to CMPs. Organizations are liable for their employees' and other agents' acts "in accordance with the federal common law of agency." This liability probably extends to BAs which are acting as agents.

For CMP purposes a "violation" is determined based on an "obligation to act or not act" under a regulatory provision, or in other words regulatory "requirements or prohibitions." Where a given requirement or prohibition is repeated in both a general and a specific form in different provisions in the same subpart, only one violation is counted. Continuing violations, such as failure to have a BAC when required, are counted as a separate violation for each day they continue.

There are four penalty tiers of penalty, as follows:

- The lowest tier provides for a minimum penalty of $100 and a maximum penalty of $50,000 per violation, for violations which the CE or BA "did not know, and by exercising reasonable diligence would not have known" about. "Reasonable diligence" is defined as "the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."

- The second tier provides for a minimum penalty of $1,000 and a maximum penalty of $50,000 per violation, for violations for "reasonable cause" which do not rise to the level of "willful neglect". "Reasonable cause" is defined in as a situation where there are "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."

- The third tier provides for a minimum penalty of $10,000 and a maximum penalty of $50,000 per violation, for violations attributed to "willful neglect". "Willful neglect" is defined as "the conscious, intentional failure or reckless indifference to the obligation to comply" with the requirement or prohibition.

- The fourth tier provides for a minimum penalty of $50,000 and a maximum penalty of $1.5 million per violation, for violations attributed to "willful neglect" that are not remedied within thirty days of the date that the CE or BA knew or should have known of the violation.

- All tiers are subject to a maximum penalty of $1,500,000 for violations of identical requirements or prohibitions during a calendar year.

These provisions are summarized in the following table.

Table 1 – Categories of Violations and Respective Penalty Amounts Available		
Violation Category	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100 - $50,000	$1,500,000
(B) Reasonable Cause	$1,000 - $50,000	$1,500,000
(C) Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
(D) Willful Neglect - Corrected	$50,000	$1,500,000

Factors affecting the possible penalty amount for each violation include the following:

- "The nature of the violation, in light of the purpose of the rule violated.
- "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."
- "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."
- "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."
- "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."
- "Such other matters as justice may require."

Civil penalties may not be imposed for an act which may be punishable under the HIPAA criminal penalty provisions, which the CE or BA has the burden of raising and proving as an

affirmative defense. A CE or BA may also affirmatively defend itself by proving that a violation was "not due to willful neglect" and corrected either within 30 days of the first date on which the CE or BA "knew, or by exercising reasonable diligence would have known, that the violation occurred," subject to extension at DHHS discretion.

The following examples demonstrate how violations may be determined.

Example 1: Unauthorized access to PHI

- BA allows unauthorized employee to access PHI on 20 individuals in a single computer file
- Unauthorized access to PHI of 20 individuals = 20 violations
- If BA could not have known about this violation in the exercise of due diligence (which seems unlikely): $100/violation = $2,000 penalty
- If BA permitted this due to reasonable cause (it is not clear this would be possible): $1,000/violation = $20,000 penalty
- If BA permitted this due to willful neglect (was recklessly indifferent to employee access activities): $500,000/violation = $1.5 million penalty ($10 million, capped)

Example 1 variation: Assume unauthorized access is discovered during log review as part of OCR investigation of unrelated complaint two years after event

- BA failed to notify CE for two years
    - One or 20 separate continuing violations? 730 violations (2 x 360) or 14,600 violations (2 x 365 x 20)
    - BA failed to notify OCR within 60 days of end of calendar year of breach
        - One continuing violation for ten months: 300 violations
        - "Could not have known:" Probably not acceptable
        - "Reasonable cause:" Probably not acceptable
        - Willful neglect, not corrected: $500,000/violation
        - $3 million penalty
        - 730 x $500,00 = $3.65 **b**illion, capped at $1.5 million
        - 300 x $500,000 = $1.5 **b**illion, capped at $1.5 million

Example 2: Defective business associate contract

- BA enters into five BACs with lower-tier BAs authorizing PHI uses not permitted by upstream BAC, including safeguards provision not adapted for HITECH requirements

- 5 violations each of 2 separate provisions = 10 violations
- If CE could not have known about this violation in the exercise of due diligence (which seems very unlikely): $100/violation = $1,000 penalty
- If CE permitted this due to reasonable cause (which probably is not possible): $1,000/violation = $10,000 penalty
- Probably would be held BA permitted this due to willful neglect: $500,000/violation = $1.5 million penalty
    - **10 x $500,000 = $5 million, capped at $1.5 million**
- Plus, probably at least one violation per transaction or event involving use or disclosure of PHI by lower-tier BA not authorized by violator's upstream BAC

Example 3: Negligent disposal of media

- BA re-sells 100 used computers without scrubbing hard drives containing PHI on 1,000 individuals.
- Potential violations:
    - Security Rule media re-use specification (100 violations)
        - Didn't know: $10,000
        - Reasonable cause: $100,000
        - Willful neglect: $1.5 million ($50 million, capped)
    - Security Rule information access management standard (100 or 1,000 violations ? – assume 1,000)
        - Didn't know: $10,000 ($100,000, capped)
        - Reasonable cause: $100,000 ($1 million, capped)
        - Willful neglect: $1.5 million ($50 million, capped)
    - Probable violation of BAC PHI use and disclosure prohibition (1,000 violations)
        - Didn't know: $25,000 ($100,000, capped)
        - Reasonable cause: $100,000 ($1 million, capped)
        - Willful neglect: $1.5 million ($500 million, capped)
    - Probably also presumed security breach if PHI was not properly encrypted
        - Didn't know: $25,000 ($100,000, capped)

- Reasonable cause: $100,000 ($1 million, capped)
- Willful neglect: $1.5 million ($500 million, capped)

- Total
  - – Didn't know: **$70,000**
  - – Reasonable cause: **$400,000**
  - – Willful neglect: **$6 million**

CMP Case Examples

The following are examples of OCR CMP actions:

Providence Health & Services. The first regulatory action to obtain a financial resolution for HIPAA violations occurred after the theft of computer hard drives storing unencrypted information about over two hundred thousand individuals. The health care provider gave public notice and notified DHHS and took mitigating and corrective actions. OCR and Providence entered into an agreement under which Providence undertook a corrective action plan and paid a $100,000 financial settlement (not a CMP).

Cignet Health. 41 patients of this four clinic health care provider filed complaints with OCR that Cignet would not grant them access to their records. Cignet ignored OCR's investigative requests. OCR obtained a court order for production of the records, to which Cignet responded by producing records on some 4,500 patients, rather than the relevant 41. OCR imposed CMPs of $4.3 million, largely based on continuing violations for failing to provide individuals with record access and failing to cooperate with OCR.

CVS and ***Rite Aid.*** OCR and the Federal Trade Commission ("FTC") pursued joint (but separate) actions against these pharmacy chains for disposing of health care information in unsecured dumpsters. CVS settled for $2.25 million and Rite Aid for $1 million. It is not clear how the settlement amounts were determined.

Blue Cross Blue Shield of Tennessee. This health insurer experienced the theft of 57 hard drives containing unencrypted information on over one million individuals. It agreed to a corrective action plan and a settlement payment of $1.5 million.

Phoenix Cardiac. This small physician practice permitted its physicians to use unencrypted, standard commercial email and cloud-based online calendaring for communications and scheduling which included unencrypted PHI. OCR imposed a fine of $100,000 and a corrective action plan.

A CMP Hypothetical

An understanding of the potential severity of CMPs might be helped by review of a hypothetical.

Assume the Oops! Clinic has decided to improve patient outreach (and perhaps patient care) by implementing an online portal through which patients can schedule appointments, provide

information about their health status (e.g. glucometer readings for individuals with diabetes, blood pressure readings) and arrange to pay for care. From a patient care and administrative perspective this is probably a good thing.

The Oops! security official is also the clinic's CIO, it's been a few years since he's reviewed HIPAA's security requirements, and he's under pressure to get the portal up and running. He therefore arranges to outsource the system to a third party, Inept BA LLC. Since it's a technical contract and the CFO gripes about unnecessary legal expenses, the CIO figures he can handle it within his authority and Oops! enters into a standard services agreement with Inept BA. This standard agreement does not include the required elements for a BAC.

Inept BA and the CIO implement the portal and set it up so that patients can register online using their name and address as shown in the Oops! records. 500 patients choose to do so. For convenience, the system is set up so any of the 75 members of the Oops! staff can access information in any patient's portal account. System logging is enabled but never reviewed as nobody really has the time. Secure socket layer encryption is implemented for online transmissions but stored data encryption is inconvenient and costs money and so is not implemented.

The system goes live on June 14, 2013. All appears to be going well. Then, in May 2016 the Oops! administrative systems are hacked, and the vulnerability is traced to the portal system. Because the hack affected patient financial data and other PHI, the CIO notifies the Oops! law firm, which advises him to notify OCR. He does so, and on June 14, 2012 OCR knocks on the door. The ensuing OCR investigation finds the following violations:

Requirement/Prohibition Violated	**Number of Violations**
No risk analysis	Continuing for three years = 1,095 violations
No Business Associate Contract	Continuing for three years = 1,095 violations
No minimum necessary policies for staff use of portal information	Continuing for three years = 1,095 violations
No staff training on secure portal use	Continuing for three years = 1,095 violations
No authorization procedures for staff access	Per-staff member = 75 violations
No workforce clearance procedures for staff access	Per-staff member = 75 violations
No access control processes for staff access	Per-staff member = 75 violations
No system log review	Continuing for three years? = 1,095 violations
No encryption of portal data in storage	Continuing for three years = 1,095 violations

Requirement/Prohibition Violated	**Number of Violations**
Review of logs indicate ~9,000 events of staff access to portal information	~9,000 minimum necessary violations
	~9,000 Privacy Rule “little security rule” violations
Patient registration does not provide for reliable authentication of patient users	Per-patient = 500 violations
Review of logs indicate ~2,500 events of patient user access to portal	~2,500 authentication violations
	~2,500 Privacy Rule “little security rule” violations

The estimated total number of violations therefore exceeds 31,295, of 14 different requirements or prohibitions. Aggravating factors include the fact that some of the violations certainly created the vulnerability which led to the security breach, potentially causing patients financial harm, and that inadequate staff and patient access controls could have caused inaccurate data to be used for patient care.

In the ensuing proceedings, OCR took the position that the violations were attributable to willful neglect (third or fourth tier CMPs) by both Oops! and Inept BA. Oops! and Inept BA each blamed the other, and both tried to prove the violations were really due to reasonable cause (second tier).

At best, Oops! could wind up facing CMPs on the order of $7 million, while at worst CMPs could be at least $21 million. Inept BA will get off a little more lightly, as it was not responsible for Oops! security administrative and "little security rule" violations, but still faces millions in possible CMPs.

Section 6: Determining the HITECH-Compliant Business Associate Contract Date

Business Associate Contracts which are compliant with HIPAA probably are not going to include all provisions needed to be compliant with the new HITECH requirements as well. Because a compliant Business Associate Contract is a regulatory requirement, failure to have a HITECH-Compliant Business Associate Contract as of the date such a contract is a required will expose both Covered Entity and its Business Associate, or a Business Associate and its downstream Business Associate, to civil monetary penalties.

DHHS recognized that there is some burden involved in amending existing Business Associate Contracts, and so allows for some existing contracts to be "deemed compliant." A HIPAA-Compliant Business Associate Contract which is "deemed compliant" satisfies the requirement to have a Business Associate Contract in place until the date on which the parties are required to implement a HITECH-Compliant Business Associate Contract. This status continues until the later of the date on which the contract or arrangement to which the Business Associate Contract applies is amended or renewed (if it is an automatically renewing or "evergreen" contract) or September 24, 2014. Parties to a Business Associate Contract which is "deemed compliant" therefore have an additional year to negotiate and establish a HITECH-Compliant Business Associate Contract, if the underlying agreement or arrangement is not amended or renewed.

This "deemed compliant" provision applies to Business Associate Contracts between Business Associates and Subcontractors as well as those between Covered Entities and Business Associates, but it is not clear whether this has much practical value. It must be hoped that DHHS would accept a contract between a Business Associate and a Subcontractor which met the criteria for a HIPAA-Compliant Business Associate Contract as "deemed compliant," since DHHS wrote the regulations to allow for such contracts in the first place. However, it is not clear that many contracts between Business Associates and Subcontractors are in fact fully HIPAA-compliant, since they didn't have to be. This is even more likely to be the case for Lower Tier Business Associates. As a practical matter, then, very few HIPAA-related contracts between Business Associates and Subcontractors are likely to be "deemed compliant."

The timing rules for determining which contracts are "deemed compliant" are somewhat convoluted for reasons which are not altogether clear. Regulations only become effective 60 days after they are published in the Federal Register, so a January 25 Federal Register publication date means the Megarule has an effective date of March 26. DHHS also provided for a 180 day period before compliance with the Megarule is required, giving a Compliance Date of September 23.

For whatever reason, DHHS chose the Federal Register publication date rather than the effective date as the cutoff for "deemed compliant" Business Associate Contracts. HIPAA-Compliant Business Associate Contracts which are in effect as of January 25 are therefore "deemed compliant" if they are not amended or renewed during the period between the March 26 effective date and the September 23 Compliance Date.

This leaves open the question of what happens if a Business Associate Contract is in effect as of January 25 and there is an amendment or renewal before March 26 but not between March 26 and September 23. The prudent assumption would probably be that it amendment or renewal between January 25 and March 26 would also cause a Business Associate Contract to no longer be "deemed compliant."

However, it should also be noted that there is no actual obligation to enter into or have in place a HITECH-Compliant Business Associate Contract before September 23, since there is no provision excepting the Business Associate Contract provisions from the overall Megarule Compliance Date of September 23. As a practical matter it will probably be better to use a HITECH-Compliant Business Associate Contract for any new agreements established after January 25 which will continue past September 23, since any non-compliant Business Associate Contract will have to be replaced or amended to be compliant by that date anyway.

It would probably also ideally be better to use a HITECH-Compliant Business Associate Contract for any amendments or renewals affecting existing Business Associate Contracts occurring after January 25. However, if it is not practical to do so there don't seem to be any regulatory consequences unless the non-compliant contract continues past September 23, 2013. Parties to such agreements or arrangements therefore would have until September 23, 2013 to settle on a HITECH-Compliant Business Associate Contract, if they were not able to negotiate one before.

The following rules therefore apply to the implementation of HITECH-Compliant Business Associate Contracts:

1. If the parties have a HIPAA-Compliant Business Associate Contract which is:
    a. In effect as of January 25, 2013, and
    b. Not renewed or modified from March 26, 2013 through September 22, 2013,
    c. That Business Associate Contract is "deemed compliant" and a HITECH-Compliant Business Associate Contract will not be required until the earlier of:
        (i) The date on which the agreement or arrangement it applies to is renewed or amended on or after September 22, 2013, or
        (ii) September 24, 2014.
2. While it is not altogether clear it appears that if the parties have a HIPAA-Compliant Business Associate Contract which is:
    a. In effect as of January 25, 2013, and
    b. The agreement or arrangement it applies to is renewed or modified between January 25, 2013 and March 25, 2013, then
    c. A HITECH-Compliant Business Associate Contract will be required as of September 23, 2013.
3. If the parties have a HIPAA-Compliant Business Associate Contract which is:
    a. In effect as of January 25, 2013, and
    b. The agreement or arrangement it applies to is renewed or modified after March 25, 2013, then
    c. A HITECH-Compliant Business Associate Contract will be required as September 23, 2013.
4. If the parties have a HIPAA-Compliant Business Associate Contract which:

   a. Applies to an agreement or arrangement which is established after January 25, then
   b. A HITECH-Compliant Business Associate Contract will be required as September 23, 2013.

5. If a Covered Entity and Business Associate have a Business Associate Contract which:
   a. Applies to an agreement or arrangement which is established after March 26, then
   b. A HITECH-Compliant Business Associate Contract will be required as September 23, 2013.
6. A HITECH-Compliant Business Associate Contract will be required for any agreement or arrangement not subject to a "deemed compliant" HIPAA-Compliant Business Associate Contract established on or after September 23, 2013.

All Business Associate Contracts will need to be HITECH-Compliant as of September 24, 2014.

Section 8: Contents of a HITECH-Compliant Business Associate Contract

NOTE: In general, this discussion applies also to group health plan documentation and arrangements between governmental entities. However, each of these has a few specific wrinkles which for simplicity's sake will not be covered here.

The good news for Covered Entities and First Tier Business Associates with existing Business Associate Contracts is that there really aren't very many differences between a HIPAA-Compliant Business Associate Contract and a HITECH-Compliant Business Associate Contract.

This is probably not as good news for most organizations contracting downstream from the first tier, where contracts consistent with the Business Associate Contract requirements have not necessarily been used. Parties to agreements or arrangements at this level will probably all too often have to negotiate more or less from scratch, but at least they will have the advantage of the previous experience of Covered Entities and First Tier Business Associates.

One potentially confusing element of the revised Business Associate Contract rule is that the implementation specifications for the contract form refer to a contract between a Covered Entity and a Business Associate. This is solved by a subsequent specification which specifies that the Business Associate Contract implementation specification applies between Business Associates and Subcontractors as well.

The original version of the rule applied only to Covered Entities, and required the Covered Entity to implement a Business Associate Contract before permitting a Business Associate to "create or receive" PHI. The revised version applies to both Covered Entities and Business Associates, and requires them to have Business Associate Contracts before they allow a downstream entity to "create, receive, **maintain or transmit**" PHI. (Emphasis added.)

In both cases, consistently with the original version, the upstream entity will be in violation of the regulations if it "knows" of "a pattern of activity or practice" which "constitutes a material breach or violation" of the Business Associate Contract, and fails to either take "reasonable steps to cure the breach," or terminates the contract. The original version, however, allowed a Covered Entity to notify DHHS if it couldn't get the breach cured and it wasn't "feasible" to terminate the contract. This alternative was deleted from the revised rule, on the theory that DHHS now has jurisdiction over Business Associates and can intervene on its own authority.

What the Megarule Changed in Business Associate Contract Content.

The only differences in the regulatory requirements for HIPAA-Compliant Business Associate Contracts and HITECH-Compliant Business Associate Contracts are the following:

- For any agreement or arrangement where a downstream entity is "carrying out" a "Covered Entity's [or upstream Business Associate's?] obligation" under the HIPAA/HITECH regulations, the downstream entity must comply with the HIPAA/HITECH requirements which would apply to the Covered Entity (or upstream Business Associate?) in performing the obligation.

  This provision is probably intended to ensure that downstream Business Associates performing Covered Entity functions governed by Privacy Rule requirements which do not apply directly to Business Associates are made applicable by contract. For example, a

downstream Business Associate EHR services vendor has agreed to be the access point for individuals wanting copies of their medical records, the vendor has to comply with an upstream hospital Covered Entity's obligation to provide it in electronic format upon request, under the time limits which would apply to the Covered Entity. In the absence of this requirement the Business Associate would not be subject to such requirements.

This suggests that whenever a downstream entity is performing a function which is governed by the Privacy Rule, the Business Associate Contract should specify the standards for its performance consistently with the regulatory requirements. I would also be concerned this might have some unintended consequences, which will show up in unexpected ways and pose annoying but hopefully reasonably solvable problems.

- The contract must require the downstream entity to comply with the Security Rule, rather than simply requiring it to "implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the Covered Entity." In practical terms this means the contract requires the downstream entity to comply with the documentation and organizational requirements of the Security Rule in addition to the safeguards requirements, consistently with the direct regulatory obligation under the new rules.
- The contract must require the downstream entity to report security breaches as well as security incidents. Business Associates have already been required to do so under the Security Breach Notification Rule. Opening up the incident reporting provisions of a Business Associate Contract for amendment to add breaches may in some (many?) cases lead to negotiations about indemnification for breach response and notification cost indemnification and possibly other remedies, which might be difficult for some parties.
- It should be noted that while this is not specified in the regulations, the DHHS discussion in the Preamble indicates that downstream Business Associate Contracts need not include the same use and disclosure permissions as apply to an upstream Business Associate, but may be the same as or "more stringent" than those requirements.

Summary of HITECH-Compliant Business Associate Contract Content.

A HITECH-Compliant Business Associate Contract must (or in some case may) have the following provisions:

1. A provision which establishes the permitted and required uses and disclosures of PHI, which does not authorize the downstream Business Associate to use or further disclose the PHI in a manner which would violate the HIPAA/HITECH rules if done by the upstream entity.
2. Optionally, a provision which permits the downstream Business Associate to use PHI for its own "proper management and administration."
3. Optionally, a provision which permits the downstream Business Associate to use PHI in order to carry out the Business Associate's own "legal responsibilities."

4. Optionally, a provision which permits the downstream Business Associate to use PHI to provide data aggregation services for purposes of the Covered Entity at the top of the contract chain.
5. Optionally, a provision permitting the downstream Business Associate to disclose PHI to carry out the Business Associate's "legal responsibilities" if "required by law."
6. Optionally, a provision permitting the downstream Business Associate to disclose PHI for purposes of its own "proper management and administration," to a person from whom the Business Associate obtains "reasonable assurances" that –
    a. The PHI will be "held confidentially;"
    b. The PHI will only be used or further disclosed as "required by law" or for the purposes for which the PHI was disclosed to the person
    c. The person will notify the Business Associate of "any instances of which it is aware in which the confidentiality of the PHI has been breached
    d. The person will implement "reasonable and appropriate security measures to protect the information."
7. A provision prohibiting the downstream Business Associate from using or further disclosing PHI other than as permitted or required by the contract or as required by law.
8. A provision requiring the downstream Business Associate to ensure that it has a compliant Business Associate Contract with any further downstream entity with which it agrees or arranges to have it create, receive, maintain, or transmit PHI for purposes, functions or services for or on behalf of a Covered Entity at the top of the contract chain.
9. A provision requiring the downstream Business Associate to comply with the Security Rule.
10. A provision requiring the downstream Business Associate to report security incidents, as well as "breaches of unsecured PHI" subject to the Security Breach Notification Rule, to the upstream entity. This provision in particular should have careful attention to make sure reporting time periods and content are consistent with Security Breach Notification Rule compliance, which may be especially problematic for Business Associates far down a Business Associate Contract chain.
11. A provision requiring the downstream Business Associate to accept restrictions on the use or disclosure of PHI which have been agreed to by the Covered Entity at the top of the contract chain.
12. A provision requiring the downstream Business Associate to make PHI available to individuals consistently with the obligation of the Covered Entity at the top of the contract chain.
13. A provision requiring the downstream Business Associate to amend or incorporate the amendment of PHI consistently with the obligations of the Covered Entity at the top of the contract chain.

14. A provision requiring the downstream Business Associate to make information available for an accounting of disclosures by or for the Covered Entity at the top of the contract chain.
15. If the downstream Business Associate is carrying out a Covered Entity's obligation governed by the Privacy Rule, in particular (but perhaps not limited to) one of the activities identified in Sections 11, 12, 13 and 14 above, to comply with the HIPAA/HITECH requirements which would apply to the Covered Entity at the top of the contract chain.
16. A provision requiring the downstream Business Associate to make its "internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of" a Covered Entity available to DHHS "for purposes of determining the Covered Entity's compliance" with HIPAA/HITECH.

    It is not clear to me that this provision shouldn't have been amended to provide that this access should apply to an investigation of either the Covered Entity at the top of the contract chain as well as the upstream Business Associate, but it wasn't. I'm not sure this has any practical implications, since Business Associates are directly subject to this requirement by regulation anyway.
17. A provision that when the Business Associate Contract terminates, "if feasible," the downstream Business Associate will return or destroy all PHI subject to the Business Associate Contract, or if that is not "feasible," will "extend the protections of the Business Associate Contract to the PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible."
18. A provision authorizing termination of the Business Associate Contract by the upstream entity, if there upstream entity determines that the downstream Business Associate has violated a material term of the Business Associate Contract.

OCR Sample Business Associate Contract

OCR has posted "Sample Business Associate Contract Provisions" with some discussion on its website. My impression is that they are a good starting point, and definitely better than the sample provided with the original Privacy Rule. It should help standardize Business Associate Contracts and reduce some negotiating and drafting disputes, which is a good thing.

However, this is a demonstration sample, not a required form. I expect some will take this as the required form and content of a Business Associate Contract, as occurred with the original sample. Over the years I've periodically run into avoidable trouble where parties adopted the sample verbatim and it didn't actually work for them. So as noted, I would take this as a starting point while considering carefully how it would actually work for any specific arrangement. In fact, I will be working on exactly that.

I've reprinted them here (no copyright claimed in these U.S. Government materials):

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA 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) Business Associate. "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].

(b) 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].

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

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) 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 protected health information other than as provided for by the Agreement;

(c) 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 parties may wish to add additional specificity 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.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) 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 parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will

forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible 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.]

Term and Termination

(a) 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.

(b) 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.]

(c) 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]

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]

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:

- 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;

- 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;

- 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.

- 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

- 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.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Section 8: Limitations on Business Associate Remuneration for Services

The healthcare sector is subject to a number of complex, overlapping and often confusing laws and regulations controlling the terms and conditions under which healthcare organizations can pay or be paid fees or receive benefits or other incentives, generally called "remuneration" for these purposes. Some of these requirements and prohibitions are counterintuitive or contrary to accepted, fully legal practices in other sectors, and some of them – the federal "Stark" and "antikickback" laws in particular – impose severe civil and criminal penalties for their violations. Anyone not familiar with these laws - perhaps Business Associates new to their role in healthcare in particular – should be sure their financial arrangements and incentive structures are compliant with these requirements.

HITECH and the Megarule have added yet another layer of complexity and risk. HITECH prohibits the "sale" of PHI. The Megarule then interpreted "sale of PHI" to mean:

> A disclosure of PHI by a Covered Entity or Business Associate, where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

"Sale of PHI" does not include disclosures of PHI which entail:

- Remuneration for legitimate public health purposes.
- Remuneration for research purposes, as defined under the Privacy Rule, limited to "a reasonable cost-based fee to cover the cost to prepare and transmit the PHI."
- Remuneration for treatment and payment purposes, as defined under the Privacy Rule.
- Remuneration for the sale, transfer, merger, or consolidation of all or part of the Covered Entity and for related due diligence, as part of health care operations.
- Remuneration to or by a Business Associate for activities that the Business Associate undertakes on behalf of an upstream Covered Entity or Business Associate, where the only remuneration provided is by the upstream entity to the Business Associate for the performance of such activities.
- Reasonable remuneration by an individual for PHI access or copying.
- Remuneration when the disclosure is required by law as permitted under the Privacy Rule.
- Remuneration for any other purpose permitted by and in accordance with the Privacy Rule, limited to a "reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose" or a fee "otherwise expressly permitted by other law."

For most Business Associate purposes one or more of these exceptions should apply, probably most often the exception for "activities that the Business Associate undertakes" on behalf of the upstream entity.

It should be noted, however, that the only exception which seems to apply to agreements or arrangements between a Business Associate and a non-Business Associate contractor, for purposes of the Business Associate's "proper management administration" is the exception for

"purposes permitted by the Privacy Rule." In that case, to the extent remuneration is provided to the Business Associate for PHI disclosed to the contractor, it will have to be reasonable, and based on the cost of preparing and transmitting the PHI for the purpose.

This should not ordinarily be an issue, unless the contractor is (for example) providing the Business Associate with a discount for rules-based care coordination support services because the Business Associate is providing the contractor with PHI so the contractor can develop or refine such rules for its own benefit. That would be a prohibited "sale of PHI."

This kind of analysis suggests that in any arrangement where a contractor provides something like a volume-based incentive for transactions or records involving PHI, the parties should document that the incentive is not based on the PHI but on other factors, such as volume-based efficiencies.

Section 10: Implications for Health Information (Exchange) Organizations

The Megarule expanded the definition of Business Associate to expressly include any "Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information."

The Megarule did not provide any definition of "Health Information Organization," (HIO) but in discussing it in the Preamble to the Rule DHHS made it clear this is to be interpreted broadly, to include regional health information organizations (RHIO) and other related types of entity, and that in any case HIOs and E-prescribing Gateways were identified only as examples of data transmission services providers, not as limitations on the definition.

The significant limitation on this definition is that it does not apply to organizations which are "conduits," i.e., which provide data transmission services that do not entail access to PHI on a routine basis. DHHS indicated that this is intended as a narrow exception:

> . . . The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to protected health information would not qualify the company as a business associate. In contrast, an entity that requires access to protected health information in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of protected health information through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate. . . .

A service can qualify as a conduit if its data transmission service is on a store-and-forward basis, as long as the storage is "temporary" or "transient." "Persistent" storage will trigger Business Associate status, if the service "has access to" PHI, "even if the entity does not view the information or only does so on a random or infrequent basis.

This last comment suggests that access controls preventing service organization access to PHI would keep it from being a Business Associate, but DHHS has provided no additional guidance on this point. If this is a valid interpretation, adequate access control might include data encryption using a methodology which would render the data "secured" for purposes of the breach notification rule, as long as the services provider doesn't have access to the encryption keys.

Entities providing data transmission services, whether identified as HIOs or otherwise, should therefore assume they are Business Associates unless their services are limited to "pure" data transmission, or if some "persistent" storage is involved, for example in a repository, if all PHI is properly encrypted and the services provider cannot access the encryption keys.

Section 10: Implications for EHR Vendors and Other Application and IT Services Providers

There are a number of models for the provision of electronic health record (EHR), personal health record (PHR), billing and administrative and related types of information system in healthcare. Whether or not a vendor of such a system depends very much on the business model used.

At one end of the spectrum the vendor may simply sell software and nothing more. In such a case the vendor is clearly **not** a Business Associate, as the sale of software should not entail any use or disclosure of PHI by the vendor.

At the other end of the spectrum a vendor may provide fully outsourced application services and even some IT staff to support operations. A full-service application services provider (ASP), whose staff need routine access to PHI to provide the services, just as clearly **is** a Business Associate.

ASPs as Conduits

Most vendors fall somewhere in between these examples, and for them the question of Business Associate status is fact-specific. Any vendor whose staff has routine or recurring access to PHI, for example to provide support, help desk or operational services, will be a Business Associate. So will any vendor which hosts or operates applications which "persistently" store PHI, or otherwise provides a PHI storage service.

This analysis follows DHHS' comments on "conduit" status. (See Section 10 for more information.) A "conduit" is an entity whose services do not entail "routine access to PHI, such as an Internet services provider (ISP).

DHHS' comments on the Megarule indicate very clearly that anything more than "transient" or "temporary" storage triggers Business Associate status if the vendor has "access" to the PHI. This suggests that access controls preventing vendor access to PHI would keep it from being a Business Associate, but DHHS has provided no additional guidance on this point. If this is a valid interpretation, adequate access control might include data encryption using a methodology which would render the data "secured" for purposes of the breach notification rule, as long as the services provider doesn't have access to the encryption keys.

Personal Health Records Vendors

The Megarule also has provisions specific to PHR vendors:

> [D]etermining whether a personal health record vendor is a business associate is a fact specific determination. A personal health record vendor is not a business associate of a covered entity solely by virtue of entering into an interoperability relationship with a covered entity. For example, when a personal health record vendor and a covered entity establish the electronic means for a covered entity's electronic health record to send protected health information to the personal health record vendor pursuant to the individual's written authorization, it does not mean that the personal health record vendor is offering the personal health record on behalf of the covered entity, even if there is an agreement between the personal health record vendor and the covered entity governing

> the exchange of data (such as an agreement specifying the technical specifications for exchanging of data or specifying that such data shall be kept confidential). In contrast, when a covered entity hires a vendor to provide and manage a personal health record service the covered entity wishes to offer its patients or enrollees, and provides the vendor with access to protected health information in order to do so, the personal health record vendor is a business associate.
>
> A personal health record vendor may offer personal health records directly to individuals and may also offer personal health records on behalf of covered entities. In such cases, the personal health record vendor is only subject to HIPAA as a business associate with respect to personal health records that are offered to individuals on behalf of covered entities.

DHHS also clearly stated that "

> a. personal health record vendor that offers a personal health record to a patient on behalf of a covered entity does not act merely as a conduit. Rather, the personal health record vendor is maintaining protected health information on behalf of the covered entity (for the benefit of the individual). Further, a personal health record vendor that operates a personal health record on behalf of a covered entity is a business associate if it has access to protected health information, regardless of whether the personal health record vendor actually exercises this access.

Entities providing application services which include any "persistent" storage of PHI should therefore assume they are Business Associates, unless their services do not involve any routine or recurring access to the PHI and they also do not have the technical ability to access the PHI, for example if all PHI is properly encrypted and the vendor cannot access the encryption keys.

Section 11: Implications for Consultants and Other Professional Services Firms

Professional services including "legal, actuarial, accounting, consulting, data aggregation . . ., management, administrative or financial services" are expressly included in the definition of Business Associate, so there is no doubt that any professional services firm which creates, receives, maintains, or transmits PHI for services provided to a Covered Entity will be a Business Associate.

The question may be more difficult when the firm is providing services to a Business Associate, however. As discussed in Section 2, a subcontractor which provides services to a Business Associate for purposes of the Covered Entity at the top of the Business Associate chain, that subcontractor becomes the next Business Associate in the chain. On the other hand if the subcontractor provides services to a Business Associate for purposes of the Business Associate, the subcontractor does not become a Business Associate. I have suggested calling this kind of subcontractor to a Business Associate a "Business Associate Services Provider," a term which has been criticized in comments but which I'll use for now.

Spotting Potential Business Associate Status.

The distinction between Business Associate and Business Associate Services Provider status can have significant implications for how a client or engagement is managed. The determination which status applies depends upon careful analysis of the intended purpose and uses of the services. This might be best shown by some examples.

Consider a hospital (Covered Entity), which contracts with a health information exchange organization (HIO) to provide health information exchange services. The HIO would be the hospital's Business Associate, and a First Tier Business Associate. The HIO might in turn contract with a different company to host and manage the record locator service used for its health information exchange services. Because the record locator service uses PHI and is part of the set of services provided by the First Tier Business Associate to the Covered Entity, the record locator service host is a Second Tier Business Associate.

Now let's take this example in a couple of different directions. The record locator service may want to contract with a consulting firm to help it develop more effective protocols for responding to record queries. Since these protocols are to be used in a service which is part of the set of services ultimately being provided to the Covered Entity, the consulting firm would become the Business Associate of the Second Tier Business Associate. This would require a Business Associate Contract between the record locator service and the consulting firm, and the consulting firm would have to fully comply with Business Associate regulatory requirements.

On the other hand, the record locator service might experience a security breach affecting the PHI in the record locator service. In that case it is likely to want legal counsel and a computer forensics firm to help it determine the scope of the breach and appropriate responses. I generally advise that in cases like this the investigation should be conducted by the forensics firm as a contractor to a law firm to get the benefits of attorney-client and work product privileges, so this Second Tier Business Associate would contract with the law firm as a Business Associate Services Provider.

The record locator service would be permitted to let the law firm have access to PHI for this purpose as part of its "proper management and administration" and in order to "carry out its legal responsibilities," as long as that was authorized under its Business Associate Contract with the HIO. (NOTE: Failure to include such a provision could therefore cause serious problems for downstream Business Associates!)

As opposed to the Business Associate Contract required for the consulting firm providing protocol advice, the record locator service would only have to have assurances from the law firm that it would hold the PHI confidentially, implement reasonable and appropriate security safeguards for the PHI, report breaches of confidentiality, and only use or further disclose the PHI for the purposes for which it was made available or as required by law. The law firm would not be considered a Business Associate and so would not be subject to Business Associate regulatory requirements, and could subcontract for computer forensics services for use in its engagement by the record locator service without the forensics firm being deemed a Business Associate.

Managing Compliance Obligations.

Business Associate regulatory compliance obligations may conflict with ethical obligations of some professional services providers, particularly law and accounting firms, but those considerations are beyond the scope of this Section. (Please contact me if you would like a copy of presentation materials on the ethical implications of Business Associate status for law firms under HITECH.) In a firm with multiple service areas they may also be hard to explain or justify to principals in non-health care practice areas, as they create firm-wide legal exposures and may require some changes to management, administrative procedures and information system configuration.

One strategy for this kind of risk and compliance management is based on the "hybrid entity" concept. Under HIPAA a hybrid entity is Covered Entity which is a single legal entity, whose business activities include both covered and non-covered functions. This kind of entity can designate "health care components," in which case the Security and Privacy Rules apply only to the health care component. Health care components include organizational units to the extent that they perform Covered Entity functions, as well as functions which would make the unit a Business Associate of a unit performing Covered Entity functions.

The Megarule commentary indicated that a commenter had suggested the regulations permit a Business Associate to designate health care components. This suggestion was dismissed with the comment that:

> As a business associate is only subject to the HIPAA Rules with respect to the protected health information it maintains, uses, or discloses on behalf of a covered entity (or business associate) and not to other information it may maintain, including health information, there is no need for business associate to designate one or more health care components.

The rules therefore did not include such a provision.

It is not clear why this distinction is supposed to be significant, since a Covered Entity is also only subject to the HIPAA rules with respect to PHI and "not to other information it may maintain." At the same time there do seem to be potential compliance and risk management

benefits for a professional services firm which has multiple practice areas, including a health care department which needs to use and disclose PHI to provide its services, to designate that department as a defined health care component. This would limit the scope of security policies and procedures and other compliance obligations to members of that department and its support staff. This may not have been positively allowed for in the Megarule, but it also was not prohibited (and perhaps not understood).

Section 12 New Healthcare Regulatory Risks for Cloud Providers; or, How to Become a Business Associate without Even Trying – or Knowing It

One of the key problem areas for cloud services providers to healthcare organizations is their status under HIPAA/HITECH: Are they Business Associates? Or aren't they?

Before the release of the HITECH Megarule my own interpretation – which was shared by a number of others - was that the Business Associate (or Business Associate subcontractor) status of a cloud-based services should depend on whether or not the vendor accessed Protected Health Information in the course of providing functions or activities for or on behalf of, or services to, a Covered Entity (or Business Associate in the case of a subcontractor). I based this interpretation on the "conduit" concept which was introduced by the U.S. Department of Health and Human Services Office of Civil Rights ("OCR") in 2000, as well as a 2003 "clarification" letter from OCR to a document storage company, from 2003.

A Short History of the HIPAA Conduit Concept.

The conduit concept was based on an analogy to the U.S. Postal Service, which transmits its senders' information in sealed envelopes which it cannot legally open without a warrant, whose contents it otherwise only accesses in non-routine circumstances such as damage to an envelope. This analogy was introduced in the preamble to the 2000 version of the Privacy Rule, with minimal discussion and no real analysis.[23] The only possible application it noted was to the "electronic equivalents" of the Postal Service.[24]

The 2000 interpretation can be summarized as follows:

- A "conduit" is defined as an entity which –
    - Transports information including Protected Health Information for or on behalf of a Covered Entity, but
    - Does not access the information other than on a random or infrequent basis,
    - As necessary for the performance of the transportation service, or
    - As required by law, where
- No disclosure of Protected Health Information to the services provider was intended by the Covered Entity, and
- The probability of exposure of any particular set of Protected Health Information is very small.

[23] U.S. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information; Final Rule*, 65 Fed.Reg. 82462 (December 28, 2000)("Privacy Rule Preamble") at 82476.

[24] Id.

This interpretation appeared to have been applied to data storage as well in a 2003 letter from OCR to Tindall Record Storage, clarifying "when a business associate agreement is required for a covered entity to enlist the services of a document and record storage company for purposes of storing [Protected Health Information:]"

> We confirm that a business associate agreement is not required between a covered entity and a document storage company performing functions on behalf of the covered entity, where any protected health information released to the storage company is transferred and maintained in closed and sealed containers, and the document storage company does not otherwise access the protected health information. Neither is a business associate agreement needed when, in these circumstances, any access to the information is merely incidental. For example, a storage company may have incidental access to protected health information if a box becomes damaged and needs to be repackaged.[25]

So how far did the conduit concept extend? Certainly it was clear that Internet services providers ("ISPs") providing messaging services, as well as other kinds of "pure" message and transaction transmission services, fell within the concept. However, since 2000 there has been a proliferation of IT solutions in healthcare, from applications and services promoted by Congress and DHHS such as electronic health records and health information exchange, to improved, more cost-effective outsourcing including cloud-based and other application services providers.

Among some lawyers helping clients develop or acquire such services, and in a number of informal as specialist listservs, there have been fairly frequent discussions about this problem, since the question whether a given service was or was not a Business Associate could clearly have significant consequences. The factors used to define and justify the 2000 interpretation factors extended quite logically to non-transmission services which store, and perhaps to some which to a limited extent process, Protected Health Information.

Coupled with the Tindall Record Storage letter, there seemed to be good reason to believe that the conduit analysis (if not necessarily the term "conduit") should apply to at least some kinds of services which stored, and perhaps in some cases to some degree processed, data including Protected Health Information. The data would not necessarily have to be encrypted with the keys unavailable to the vendor – i.e., it would not have to actually be impossible for the vendor to access the Protected Health Information – as long as access was not part of the services and was otherwise random and infrequent and the potential for unauthorized access, use or disclosure was sufficiently low.

[25] Letter from Richard M. Campanelli, Director, OCR, to Ms. Elizabeth Tindall (May 12, 2003).

OCR did not amplify or explain its analysis of this concept until the HITECH Megarule. The 2010 Notice of Proposed Rulemaking for the regulations which became the Megarule mentioned the conduit concept only in passing, noting a change required by the HITECH Act:

> . . . data transmission organizations that the {HITECH] Act requires to be treated as Business Associates are those that require access to Protected 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.[26]

There was no indication OCR was considering changing the 2000 interpretation. In the 305 comments on the NPRM the only comments specifically addressing the issue were from AT&T, which was principally concerned that use of its data transmission services not trigger Business Associate status,[27] and from Tindall Record Storage, which requested clarification

> . . . that box and file level off-site storage of property (that may contain PHI) of potential "covered entity" clients be formally characterized as a "conduit" function that does not subject the storage company to the operation of HIPAA and its progeny. Secondarily, insofar as any service performed by a storage company might require execution of a business associate agreement, please clarify that inclusion of an indemnity is outside the purview of HIPAA and its progeny.[28]

Aside from these comments, a couple of technology industry associations expressed concern that Business Associate status would be triggered unexpectedly for some companies, but their comments provided no real details or meaningful description of technologies or arrangements be implicated.

Limitation of the Conduit Concept under the HITECH Rules.

In the preamble to the Megarule, OCR expressly declined to extend the conduit concept to document storage and related types of service. The regulations themselves do not specifically address this issue, but the interpretation in the preamble makes it clear the conduit exception is

---

[26] U.S. Department of Health and Human Services Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed.Reg. 40868 (July 14, 2010) at 40873.

[27] Letter from Keith Krom, Vice-President and General Counsel – Washington, AT&T to OCR, ATTN: HITECH Privacy and Security Rules Modifications (September 13, 2010).

[28] Letter from Elizabeth Tindall, General Counsel, to OCR, Attention: HITECH Privacy and Security Ru1e Modifications (September 1, 2010). Interestingly, 36 comments (almost 12% of all comments) were from document storage companies, apparently principally or entirely hard-copy document storage, as well as their trade association. These comments were principally, and in most cases entirely, concerned with Covered Entity demands for indemnification against security breaches by such companies storing their records, but a number did request express extension of the conduit concept to such companies, as did a comment with respect to personal health records.

not intended to apply beyond data transmission services. In particular, this interpretation states that "data transmission organizations that do not require access to Protected Health Information on a routine basis would not be treated as Business Associates", and that the conduit

> . . . determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to Protected Health Information to perform the service for the Covered Entity. The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services.[29]

The discussion then reiterates that the conduit exception "is limited to transmission services . . . including any temporary storage of transmitted data incident to such transmission."[30]

On the other hand, "an entity that maintains Protected Health Information on behalf of a Covered Entity is a Business Associate and not a conduit, even if the entity does not actually view the Protected Health Information."[31] This distinction is stated to be based on the

> . . . transient versus persistent nature of that opportunity [for the entity to access the Protected Health Information]. For example, a data storage company that has access to protected health information qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold.[32]

For this reason the definition of Business Associate was expanded to clarify that it includes entities which "maintain" Protected Health Information on behalf of a Covered Entity.[33] Specifically, "a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis."[34]

---

[29] U.S. 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, 78 Fed.Reg. 5566 (January 25, 2013)("Megarule") at 5571.

[30] Id. At 5572.

[31] Id.

[32] Id.

[33] Id.

[34] Id.

This interpretation is inconsistent with the Tindall Record Storage letter interpretation. For electronic Protected Health Information, the Security Rule provides a definition of "access" as "the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource."[35] The HITECH preamble interpretation therefore appears to mean that access controls which actually preclude vendor access to data – e.g., encryption without vendor access to the keys – is necessary for the vendor to avoid Business Associate status.

Even this interpretation, however, seems looser than an interpretation apparently given by an OCR official in at least one presentation. I am told – I was unable to attend the presentation myself[36] - that this interpretation was that a vendor storing electronic Protected Health Information is a Business Associate even if the data is encrypted and the vendor doesn't have access to the encryption keys. The basis for this interpretation apparently was that encrypted or not, the vendor is "maintaining" the Protected Health Information. I don't know how the issue was presented, but this interpretation would be inconsistent with the interpretation in the preamble to the Megarule. Since this was a comment at an educational event it shouldn't be taken as the official OCR position, and may be an error or misstatement, or based on a misunderstanding of a question. It would, however, be very helpful for OCR to issue a well-advised clarification for the reasons discussed below.

Problems with the New Interpretation.

The implications of the new interpretation may be a problem and something of a surprise to some cloud and application services providers. The problem is that Business Associate status and liability attach automatically when an entity obtains Protected Health Information for a purpose of a Covered Entity, even indirectly from or for a Business Associate – not upon entry into a Business Associate Contract or with any formal notice.[37] This means that even a services provider which doesn't control what users upload and has no way of knowing what it is storing automatically becomes a Business Associate – with no Business Associate Contracts and without ever knowing it.

Consider for example Dropbox, which per Wikipedia is a free

> . . . file hosting service operated by Dropbox, Inc., that offers cloud storage, file synchronization, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronises so that it appears to be the

[35] 45 C.F.R. § 164.304.

[36] American Bar Association Health Law Section and Center for Professional Development, *Cutting through the HIPAA Hype: What You Need to Know About the HITECH Act Rules* (January 25, 2013)

[37] Megarule at 5598.

> same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications.[38]

Under the new interpretation if, say, a physician practice (Covered Entity) or practice management services vendor (Business Associate) were to use a service like Dropbox as backup storage, that service would be automatically become a Business Associate, without notice, even if the practice or services vendor encrypted the Protected Health Information.

DHHS has already penalized a physician practice for storing unencrypted data in a cloud-based calendar service,[39] and presumably under the new rules both the practice and the vendor could be penalized. Violations by the hosting service in this kind of scenario would include not only a wide range of compliance failures, including failure to have a Business Associate Contract.

It is also well worth noting that the "transient" versus "persistent" storage distinction which is supposed to differentiate Business Associate "storage" services from non-Business Associate "transmission" services doesn't necessarily reflect all "transmission" models. Quite a few ISPs offer email services which include storage on the ISP's servers for very long periods of time – "persistent" storage for periods determined by the user. While it may be true that Covered Entities (and Business Associates) shouldn't transmit (and therefore potentially store) unencrypted email which includes Protected Health Information,[40] if one does then under this analysis the ISP automatically becomes a Business Associate. The sender more than likely violated the Security Rule in doing so, but under this analysis that is irrelevant: The fact that the ISP is "maintaining" Protected Health Information in "persistent" storage is enough.

Conclusion.

My suspicion is that a major reason for the new interpretation is that the data storage issue was not raised very strongly or clearly, and especially lacked analytical discussion. Then again, it wasn't clear that OCR was considering a revised interpretation of the concept which would expressly exclude data storage, or what that might imply.

Of most concern is the problem of unexpected Business Associate status. This was raised in the comments on the proposed rulemaking, and not addressed by OCR. It may be that OCR assumed

---

[38] See Wikipedia, *Dropbox (Service)*, available at http://en.wikipedia.org/wiki/Dropbox_%28service%29 (visited January 25, 2013)

[39] See U.S. Department of Health and Human Services Health Information Privacy website, *HHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards*, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.html (visited January 25, 2013).

[40] See 45 C.F.R. § 164.312€(2)(ii)(Security Rule addressable specification requiring encryption of Protected Health Information in transmission "whenever deemed appropriate").

it was only a concern for data transmission services like AT&T (though the question was raised in other comments), and adequately dealt with by allowing for "random/infrequent" access to Protected Health Information. Whatever the reason, the risks associated with unanticipated, unmanaged (and possibly unknown) Business Associate status make this a difficult and unfair problem.