InfoSafe Shredding
Mobile Document Destruction
"Protecting Your Privacy"
402-891-2688

FAQ on InfoSafe Shredding Services: Frequently Asked Questions on InfoSafe Shredding
Information And Video on One Time Cleanouts: Cleanouts and Purges

Business Associates under HITECH: A Chain of Trust

The Business Associate provisions of the HITECH Megarule ("Megarule")[1] establishes 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[2] were removed by the HITECH Act. **Now the regulations apply not only to covered entities, but to any other entity which work 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.[3]**

The Megarule also extended Security Rule and select Privacy Rule obligations directly to business associates,[4] while **retaining the requirement that covered entities establish and maintain business associate contracts[5] 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.[6] 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.[7]

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.

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

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.[8]

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."[9] This means that subcontractors, which previously were only regulated second-hand by subcontractor provisions requiring business associates in general terms to pass along protection requirements,[10] 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,[11] 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,[12] 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:[13] 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.[14] 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.[15] 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 limitations at least as stringent as, and if appropriate more stringent than, its own upstream business associate contract provides.[16]

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.[17] 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.[18]

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."[19] 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.[20]

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.[21]

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 more 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.

[1] 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).

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

[3] 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.

[4] 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.

[5] "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.

[6] Megarule at 5598.

[7] 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[.]

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

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

[9] 45 C.F.R. § 160.103, as amended by the Megarule.

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

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

[12] 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.

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

[14] 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.

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

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

[17] See 45 C.F.R. § § 164.524.

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

[19] 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."

[20] 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.

[21] Megarule at 5601.