Amending Business Associate Contracts: Harmonizing Privacy and Security for Protected Health Information

by Nilay B. Patel, LLB

With the April 21, 2005, and April 20, 2006 (for small health plans) HIPAA security regulation deadlines, covered entities may question what a revised contract for a business associate (BA) should contain and how it should be executed. Official guidance is scattered in the Federal Register and contains a stream of clarifications. Revising BA contracts drafted and executed under the auspices of the HIPAA privacy regulation in 2003 may be a challenge for healthcare organizations. This article provides guidance on the substance of the amended business associate contract and the logistics of its execution.

BA Contracts and the Privacy Regulation

Under the HIPAA privacy regulation, all covered entities with business associates were required to execute BA contracts. However, the privacy regulation is more comprehensive than the security regulation in its requirements of a BA contract, and it is within the privacy infrastructure that compliance with the security regulation must be achieved.

BA Contracts and the Security Regulation

Under the security regulation, covered entities must obtain satisfactory assurances in writing from business associates that electronic protected health information (PHI) will be safeguarded. The regulation requires that the business associate will:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity
- Ensure that any agent (including a subcontractor) to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it
- Report any security incident to the covered entity
- Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract[1]

These requirements, although similar to the privacy regulation requirements, focus on security. A number of issues emanate from implementing these requirements into existing BA contracts.

Implementing New Requirements into Existing Contracts

All BA contracts were or are to be reviewed, revised, and re-executed by the security regulation compliance deadlines, with no exceptions or extensions. The privacy regulation, however, allowed a transition period where covered entities were granted one additional year for executing BA contracts subject to fulfilling certain criteria. The rationale for the transition period was to ease financial and other issues associated with renegotiating existing contracts. The absence of a transition period under the security regulation is mitigated by the fact that covered entities already have experience with BA contracts under the privacy regulation and have as such rekindled long-dormant relationships and established rapport with their business associates. As a result they have already identified and resolved some of the difficult issues with business associates. As all contractual documents were collated during implementation of the privacy regulation, making amendments to reflect the security regulation should be more efficient.

Covered entities have grappled or will be grappling with the decision between redrafting their contracts or attaching an addendum. There is no official governmental guidance on this subject.

Prior to implementation of the privacy regulation, covered entities would have had a service agreement or contract regulating disclosure or transmission of PHI. After the privacy regulation, covered entities generally had two options: include the privacy requirements in the existing service agreement, thus maintaining one all-encompassing contractual document, or create an addendum to the service agreement containing all privacy requirements, thus being regulated by two contracts.

It is recommended that the document containing the privacy requirements also contain the security requirements. Thus, for the first option above, the service agreement would contain all HIPAA terms, while in the second option the addendum would contain all HIPAA terms. The reasons for not creating a separate document solely for the security requirements include:

- Duplicity of language. The privacy regulation requires that a BA contract include a provision that the business associate report to the covered entity any use or disclosure of PHI not covered by the contract.[2] Similarly, the security regulation requires that a BA contract include a provision that the business associate report to the covered entity any security incident. With careful drafting, both requirements can be blended into one clause.
- The US Department of Health and Human Services has indicated strongly (in a different context but applicable here) that "because the purpose of the security standards is in part to reinforce privacy protections, it makes sense to align the organizational policies of the two regulations."[3]
- Increased probability of conflict or ambiguity in language among and between multiple contracts and addenda, thus invoking multiple laws relating to contract interpretation.
- The remote but plausible possibility that where a service agreement, addenda, or other arrangement appears to be comprehensive and entire, the successors to, assignees, or beneficiaries of it are unaware of all other current contractual documents.

Revising the business associate contract does not require wholesale revisions to the existing privacy framework. The table at right displays the symmetry between the privacy and security regulations.

Business associate contract provisions may be redrafted by combining the two like requirements into one single section or by creating two subsections within a section, each of which addresses one of the two like requirements.

The first requirement shown in the table could invoke the second option because the privacy requirement is directed at PHI while the security requirement is limited to electronic PHI and to combine it would result in confusion and undue verbosity.

The second requirement shown in the table may be combined into one single section as follows: "The business associate shall ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such PHI, and with respect to electronic PHI, agrees to implement reasonable and appropriate safeguards to protect it."

The third requirement may be revised to read: "The business associate will report to the covered entity any use or disclosure of PHI not provided for by the contract or any security incident involving electronic PHI, of which it becomes aware."

Finally, no changes to the existing business associate contract are required for the fourth requirement.

Simple and to the Point

When redrafting their business associate contracts, covered entities should ensure simplicity and brevity. As the Federal Register points out, "the language should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress."[4] The more detailed aspects of the security regulation are addressed in the policies and procedures that covered entities are required to maintain. Excess detail in BA contracts may result in constant amendments and re-execution, where "a covered entity may change its policies and procedures at any time."[5]

A review of existing BA contracts must also include a section of definitions. Covered entities should decide whether to include terms such as "electronic PHI," "administrative safeguards," "technical safeguards," and "physical safeguards," all of which are defined in HIPAA.[6]

When redrafting, care should be taken not to casually interchange the terms "PHI" (subject of the privacy regulation) and "electronic PHI"(subject of the privacy and security regulations), the latter of which is narrower in scope than the former. Protections that must be afforded to PHI under the privacy regulation cannot be restricted in its application to electronic PHI only.

The security regulation's notion that covered entities implement "reasonable" and "appropriate" measures should be extended to BA contracts. "Reasonableness" will be the legal touchstone in any compliance investigation. Compliance will be objectively measured against what a covered entity of the size, complexity, and capabilities of the offending covered entity would reasonably have designed and implemented.

Amending BA contracts for the security regulation is not merely adding a few provisions at the end of existing BA contracts. Security regulation requirements must be logically incorporated, and the entire contract must be reviewed in detail.

Parallel BA Requirements	
Security Rule Requirements	**Privacy Rule Counterpart**
Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI created, received, maintained, or transmitted on behalf of the covered entity.	Provide that the business associate will use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the contract.
Provide that the business associate will ensure that any agent, including a subcontractor, to whom the business associate provides electronic PHI, agrees to implement reasonable and appropriate safeguards to protect it.	Provide that the business associate will ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such PHI.
The business associate will report to the covered entity any security incident of which it becomes aware.	The business associate will report to the covered entity any use or disclosure of PHI not provided for by the contract of which it becomes aware.
Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Notes

1. "Security Standards Final Rule." 45 CFR §164.314(a)(2)(i). *Federal Register* 68, no. 34 (2003). Available online at www.hhs.gov/ocr/hipaa.
2. "Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. 45 CFR §164.504(e)(2)(ii)(C). Available online at http://aspe.hhs.gov/admnsimp.
3. *Federal Register* 68, no. 204 (2003): 8359. Available online at www.uscg.mil/hq/g-m/mp/pdf/final33cfr/ps.pdf.
4. Ibid, p. 8336.
5. "Security Standards Final Rule." 45 CFR §164.316(a).
6. "Security Standards Final Rule." 45 CFR §164.304.

Nilay B. Patel *(nbpatel1@hotmail.com) is a compliance specialist and deputy privacy officer at Care1st Health Plan in Los Angeles, CA.*

Article citation:
Patel, Nilay B. "Amending Business Associate Contracts: Harmonizing Privacy and

Security for Protected Health Information." *Journal of AHIMA* 76, no.7 (July-August 2005): 58-59.