

GUIDE TO BUSINESS ASSOCIATES

An Instructional Document Written by WorkSmart MD, Inc.

Extracted from the HIPAA Rx™ Compliance Software

The Health Insurance Portability and Accountability Act (HIPAA) is conceivably one of the most significant pieces of legislation to affect health information management in years. Not only does it impact healthcare providers, healthcare clearinghouses, and health plans, it affects all business associates that create, transmit, maintain and receive protected health information. A business associate is a person to whom a healthcare provider discloses protected health information so the person can assist or perform a function for the healthcare provider. This includes lawyers, auditors, consultants, third-party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities. Individuals who are in the workforce of a healthcare provider are not business associates. Thus, covered entities need not enter into business associate agreements with their employees.

Steps for Business Associates

Almost assuredly, under the HIPAA regulations covered entities will need to amend any business associate agreements that will be in existence on the relevant compliance date. In addition to reviewing the final rule, here are some steps that the covered entity, if it is a healthcare provider, can take to bring business associate agreements into compliance.

Step 1: Inventory all Business Associates. Determine who the covered entity's business associates are. Identify all vendors that create, maintain, transmit, receive or monitor protected health information on behalf of the covered entity. This includes protected health information in written, oral, and electronic formats. To assist you with this the HIPAA Rx software includes a business associate inventory template.

Step 2: Understand the Business Associate Requirements. The HIPAA privacy and security rule requires the covered entity to obtain satisfactory assurances that its business associates will safeguard protected health information. These assurances should be documented through business associate contracts. The HIPAA privacy and security rule outlines key terminology that should be included in the business associate contracts.

Step 3: Have Business Associates Complete Security Assessments. To ensure that business associates reasonably and appropriately safeguard protected health information the covered entity should consider having each business associate complete a "Vendor Security Assessment Questionnaire". The HIPAA Rx software includes a questionnaire in the **Assessment Tools** module.

Step 4: Customize Business Associate Contracts. In addition to existing contracts that may need to be amended, the covered entity will be entering into new agreements. The HIPAA Rx software includes a template for a business associate contract. This contract should be reviewed and customized as needed. A contract should be customized for each of the business associates identified during the inventory.

Step 5: Obtain Signatures. Once contracts are customized ensure that a principle of the organization signs the contract. Maintain all business associate contracts for at least six years.

The final HIPAA privacy rule was published on August 14, 2002 and adopted a transition period for certain business associate contracts that permits covered entities, other than small health plans, to operate under such contracts for up to a year beyond the April 14, 2003 compliance date. However, this transition period is available only to covered entities that have written contracts or other written arrangements with business associates prior to the effective date of the Final Rule, and only if those contracts or arrangements are not renewed or modified prior to April 14, 2003. This transition period was intended to afford covered entities (especially large covered entities) sufficient time to reopen and renegotiate existing contracts.

Business Associate Requirements

A healthcare provider may not disclose protected health information to a business associate without satisfactory assurance from the business associate that it will appropriately safeguard the information. This requirement does not apply to providers disclosing health information to another provider for treatment or referral purposes.

Releases of health information for reasons other than treatment, payment, or operations (e.g., for research, marketing, etc.) require a written business associate agreement. A written agreement should establish the permitted uses and disclosures of protected health information by the business associate. The HIPAA privacy and security regulations require the inclusion of some specific provisions in the agreements.

Contract Provisions

The agreement must provide that the business associate may not use or disclose the information other than as expressly permitted or required by the agreement. A simple statement to that effect in the agreement should satisfy the regulations. There should be a fairly specific description elsewhere in the agreement of how the business associate can use, and to what extent it can disclose, the protected health information.

The agreement should state that the business associate may not use or disclose the protected health information in a manner that would violate the regulations if done by the healthcare provider itself. A simple statement to that effect should satisfy the requirement.

The regulations also require a list of provisions that are fairly standard in confidentiality agreements and may therefore already be in agreements under which the healthcare provider discloses protected health information.

The agreement should require the business associate to use appropriate safeguards to prevent use or disclosure of the protected health information other than as provided for by the agreement. A simple statement to this effect should satisfy the regulations.

Another provision frequently found in confidentiality agreements and required by the regulations requires the business associate to report to the healthcare provider any use or disclosure of the protected health information in violation of the agreement of which it becomes aware. The healthcare provider may want to specify how soon after becoming aware of the breach the business associate must inform the healthcare provider. Provisions could require notice "within 24 hours," for example, or "as soon as reasonably possible." A definitive requirement like "within 24 hours" may be more desirable because it avoids a later dispute over whether the business associate has satisfied the obligation.

The business associate must ensure that any subcontractors or agents agree to the same restrictions and conditions that apply to the business associate with respect to protected health information. One relatively easy way to accomplish this is to include a provision stating that certain identified provisions should flow down to subcontractors or agents. The business associate should warrant that it will include such requirements in any subcontract or agent agreement.

The agreement must obligate the business associate to make protected health information available pursuant to section 164.514(a) ("Right of access for inspection or copying") of the HIPAA privacy regulations. This can be accomplished with a simple statement to that effect in the agreement.

The agreement must obligate the business associate to make its internal practices, books, and records relating to the use and disclosure of protected health information available to HHS for purposes of determining the healthcare provider's compliance with the privacy regulations. Again, the healthcare provider may consider closely paraphrasing the language in the regulation for this provision. Business associates, however, may want more specificity and may want to limit access in some way. The agreement should not permit restrictions on HHS' access to the point that HHS itself determines that the regulation requiring access has not been satisfied.

The agreement should also stipulate that upon termination, the business associate will return or destroy all protected health information received from the healthcare provider and will not retain copies of such information.

While not expressly required by the regulations, the agreement should also state that if the business associate chooses to destroy the protected health information, it will certify to the healthcare provider that it has done so.

Since the business associate will perform this function after termination of the agreement, there should be language that states that the provision requiring return or destruction of protected health information upon termination of the agreement would survive such termination. Otherwise, the business associates' obligation to do so arguably ends upon termination of the agreement.

When a request to correct protected health information is accepted by the healthcare provider, the entity must make reasonable efforts to notify other entities, including business associates, of the correction. The business associate agreement should obligate the business associate to incorporate any corrections to protected health information when notified of such correction by the healthcare provider.

The healthcare provider should be able to terminate the contract if the healthcare provider determines that the business associate has violated a material term of the contract. Here, the healthcare provider will almost assuredly want more specificity than that stated in the regulations. The healthcare provider will want to make it clear that:

- it can immediately terminate the agreement for material breach
- included in the definition of material breach is a breach of any of the above-referenced provisions
- the healthcare provider need not provide a cure period

The agreement should contain a provision that failure to terminate for breach in one instance does not preclude the healthcare provider from terminating the agreement for that breach at some point in the future or for any future material breach.

There should be a provision under which the business associate warrants that it will protect the integrity and availability of the protected health information. This provision could also provide specific requirements that the business associate must meet. If so, the agreement should state that the list of requirements is not exhaustive. In effect, the business associate would be required to take certain defined steps in addition to providing the aforementioned warranty.

Under the regulations, covered entities must issue a notice of privacy practices. Business associates are bound by the information practices of the healthcare provider with whom they contract. Covered entities should consider including a provision in their business associate agreements to that effect.

Business associate contracts should give the healthcare provider the right to audit and monitor the business associate to confirm compliance with the agreement and privacy regulations. (This is in addition to the required provision that allows HHS to audit the business associate.)

Business associates may try to limit healthcare provider audits to a specified number per year and may resist ongoing monitoring. A material breach by a business associate of any of the provisions required by the regulations will be considered to be noncompliance by the healthcare provider itself if the healthcare provider knew or reasonably should have known of such breach and failed to take reasonable steps to repair the breach or terminate the agreement.

The healthcare provider should anticipate breaches of the agreement by business associates and will want to be able to obtain an injunction to stop any continuing breach. Therefore, the healthcare provider will want a provision allowing it to seek an injunction as well as damages. The provision should state that the healthcare provider will not need to post bond, and the provision should state that seeking damages or an injunction is not an exclusive remedy.

Because HHS may consider a healthcare provider to be in violation of the regulations if its business associate is in violation, an entity should require very strong indemnification and "hold harmless" language in the agreement. This language should require a business associate to pay defense costs and any expenses that the entity suffers as a result of a breach of the agreement by the business associate, its employees, agents, or subcontractors. This provision should allow the healthcare provider to control its own defense and make settlements and should protect the healthcare provider's officers, employees, and agents, in addition to the healthcare provider itself.

If the healthcare provider is entering into an agreement to purchase software or hardware, the agreement should require the vendor to make any changes to the hardware or software necessitated by changes to the HIPAA regulations. Healthcare providers will want the agreement to obligate the vendor to provide appropriate products, even if the vendor decides to accommodate revisions to HIPAA with a new product rather than upgrades to existing products.

Recommendations

To ensure secure and private transactions with all affected business associates organizations should perform the following tasks:

- Identify all third party relationships
- Use best security practices for those third parties accessing protected health information on one's own host systems
- Insist on open third party site assessments, on-going compliance reporting and complete disclosure depending on the nature of the relationship
- Amend agreements to include the most stringent healthcare industry privacy policies after ensuring HIPAA compliance
- Amend all existing and interim business associate contracts to include HIPAA compliance requirements

Business associates are often critical components to the successful operations of healthcare providers. If a business associate is unable to fulfill its obligations to safeguard protected health information, the relationship with the vendor may need to be severed. It is recommended that the covered entity not become overly dependent on any business associate.

Although the covered entity is not required to monitor the activity of its business associates they are required to mitigate the harmful effects caused by their incidental and unauthorized disclosures.