

# HIPAA Compliance Questions for Business Partner Agreements

by Michael C. Roach

---

*If your organization is covered by HIPAA, do you know what's expected of you—and of your vendors—with regard to privacy of health information? To make sure your organization is in compliance, contracts with business partners will need careful review. The author offers an overview of the proposed regulations and offers some tips to get started.*

---

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. Across the country, healthcare organizations have already been discussing how to become compliant with the regulations in areas such as electronic data interchange, privacy, and security.

While HIPAA's impact will certainly be felt in medical record, billing, and reimbursement systems, other areas will be affected as well. Healthcare organizations will need to review contracts with various business partners to make sure that these, too, are in compliance. These contracts—known as "business partner agreements" will be regulated by HIPAA and will require the attention of all participants.

What are the business partner requirements? What provisions should they contain, and what should covered entities be alert for when drafting these provisions? What steps can organizations take today to get their business partner agreements in line with the regulations? This article answers these questions.

## Applicability, Definitions, and Effective Dates

HIPAA was enacted on August 21, 1996.<sup>1</sup> Subpart F of Title II of HIPAA contains the administrative simplification provisions from which the proposed privacy regulations stem.<sup>2</sup> HIPAA required the Department of Health and Human Services (HHS) to develop regulations related to privacy in the event Congress failed to enact legislation to impose recommendations made by the secretary of HHS.<sup>3</sup> The proposed privacy regulations were published in the Federal Register November 3, 1999,<sup>4</sup> and final regulations were published on December 28, 2000.

A few key terms: The regulations will apply to any entity that is a health plan, a healthcare clearinghouse, or a healthcare provider (as these terms are defined in the regulations) that electronically transmits or maintains protected health information. These are known as "covered entities" or a "covered entity."<sup>5</sup>

Another key term is "protected health information" (PHI). PHI is information that is electronically maintained or transmitted that:

- is created or received by a covered entity, public health authority, employer, life insurer, school, or university
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual
- identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual <sup>6</sup>

Finally, a "business partner" (referred to as "business associate" in the final rule) is a person to whom a covered entity discloses PHI so the person can assist or perform a function for the covered entity. This includes lawyers, auditors, consultants, third-party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities. Individuals who are in the work force of the

covered entity are not business partners.<sup>7</sup> Thus, covered entities need not enter into business partner agreements with their employees.

## How to ensure your contracts are compliant

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

**Step 1: Inventory all existing agreements.** Determine which are business partner agreements and, of those, which will be in effect on the relevant compliance date. In doing this inventory, look beyond just formal agreements to any relevant letter agreements and determine the existence, or lack thereof, of oral agreements. One way to look for evidence of oral agreements is to look for individual "consultants" or others who are performing work at or for the covered entity without a written agreement. Educate all officers—even the president or CEO—and managers who have authority to purchase services so that they do not overlook such arrangements when they are asked to produce all relevant business partner agreements. "HIPAA Contract Compliance Flow Sheet," page 48, can help a covered entity inventory its agreements.

**Step 2: Know the rules.** Make sure that the individual drafting business partner agreements has a fair understanding of the relevant HIPAA regulations. Not all contract writers or lawyers are aware that the regulations require certain provisions to be included in such agreements.

**Step 3: Draft model language.** In addition to existing contracts that may need to be amended, your organization will be entering into new agreements between now and the compliance deadline. But don't take a "cookie cutter" approach. It's one thing to have model language—it's another entirely to have language that is appropriate for the specific business deal at issue. Model language can provide a starting point for the contract drafter, but it should not be dropped into an agreement without thought to whether it is appropriate or needs to be modified for the specific deal in question.

**Step 4: Establish a work plan.** Create a work plan to enter into negotiations with business partners with whom your organization has agreements that will need to be amended. Be aware that vendors will view the provisions discussed in this article as extremely burdensome. They will almost assuredly ask for additional money in exchange for including additional provisions in the agreement. Covered entities, likewise, should be leery of adding obligations to an existing agreement without providing the business partner some form of additional consideration.

Negotiating the amendments is likely to be a time-consuming and difficult process. In some cases, the covered entity may find itself needing to terminate an existing agreement and to find an alternative source for the services. Avoid getting trapped in a situation where there is no time to take business elsewhere, thus becoming hostage to the current business partner. Along these lines, develop some exit strategies that could be put in place once a critical date is passed. For instance, if locating an alternative to an existing vendor and negotiating a new contract would take approximately five months, the covered entity is trapped if its negotiations for amendments with the existing vendor are not substantially completed five months prior to the relevant compliance date. This is especially true if the vendor knows that it will take the covered entity five months to negotiate an agreement with a replacement.

**Step 5: Look at current agreements** that will be completed by the relevant compliance date. Will the deliverable under such an agreement need to be modified to satisfy the regulations? For example, if a covered entity is currently purchasing a new information system that will be completely installed before the relevant compliance date, and if that information system will not allow the covered entity to meet the requirements of the transaction, security, and privacy regulations, changes to that agreement need to be negotiated now.

Covered entities have until February 2003 to comply with the regulations.<sup>8</sup> However, health plans with annual receipts of less than five million dollars will have an additional 12 months to become compliant.<sup>9</sup> These dates will be referred to in this article as the "compliance dates."

### **What Is Required? Reviewing Business Partner Requirements**

A covered entity may not disclose PHI to a business partner without assurance from the business partner that it will appropriately safeguard the information.<sup>10</sup> There is a narrow exception to this rule. Disclosures by a provider to another provider for consultation or referral purposes do not need to meet the business partner requirements.<sup>11</sup>

Releases for reasons other than consultation or referral (e.g., for research purposes) would require a business partner agreement. A written agreement that establishes the permitted uses and disclosures of PHI by the business partner is required.<sup>12</sup> The proposed regulations require the inclusion of some specific provisions in those agreements.

### **Contract Provisions**

#### Provisions Required By Regulation

The proposed regulations list a number of provisions that are required in the business partner agreements.<sup>13</sup> This article will discuss the requirements generally in the order presented in the regulation—not necessarily in order of importance from a legal standpoint.

First, the agreement must provide that the business partner may not use or disclose the information other than as expressly permitted or required by the agreement.<sup>14</sup> A simple statement to that effect in the agreement should satisfy the proposed regulations. Of course, there must be a fairly specific description elsewhere in the agreement of how the business partner can use, and to what extent it can disclose, the PHI.

The agreement must state that the business partner may not use or disclose the PHI in a manner that would violate the regulations if done by the covered entity itself.<sup>15</sup> Again, a simple statement to that effect should suffice to satisfy that requirement.

The proposed regulations also require a list of provisions that are fairly standard in confidentiality agreements and may therefore already be in agreements under which the covered entity discloses PHI. The agreement must require the business partner to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the agreement.<sup>16</sup> A simple statement to this effect should satisfy the proposed regulation. However, the covered entity may want to go further and specify what some of those safeguards might be.

There are different views on how to approach this type of issue, and each approach can cause its own set of problems if there is a dispute later about this provision. Some people feel a simple, general statement is too vague, and reasonable people can certainly disagree over what constitutes "appropriate safeguards." Conversely, attempting to list what steps should be taken by the business partner can lead to lengthy negotiations, may produce a list that is not appropriate for the circumstances, and may inadvertently free the business partner from implementing some safeguards it otherwise would.

Another provision frequently found in confidentiality agreements and required by the proposed regulations requires the business partner to report to the covered entity any use or disclosure of the PHI in violation of the agreement of which it becomes aware.<sup>17</sup> The covered entity may want to specify how soon after becoming aware of the breach the business partner must inform the covered entity. 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 partner has satisfied the obligation.

The business partner must ensure that any subcontractors or agents agree to the same restrictions and conditions that apply to the business partner with respect to PHI. One relatively easy way to accomplish this is to include a provision stating that certain identified provisions must flow down to

subcontractors or agents. The business partner should warrant that it will include such requirements in any subcontract or agent agreement.

The agreement must obligate the business partner to make PHI available pursuant to section 164.514(a) ("Right of access for inspection or copying") of the proposed privacy regulations.<sup>18</sup> This can be accomplished with a simple statement to that effect in the agreement.

However, the wording of the regulation raises a question—do the other provisions of proposed regulation §164.514 apply to the business partner when it comes to granting access to the PHI? For instance, §164.514(b) states that a covered entity can deny access to PHI under certain circumstances. However, the proposed regulations state only that the business partner must make the PHI available in accordance with §164.514(a). Therefore, does the limitation on access stated in §164.514(b) apply to business partners?

Likewise, it is unclear whether the other subsections of §164.514 apply to business partners. Almost assuredly, they do. It is unlikely that HHS would allow covered entities to deny access to the PHI and not allow business partners to do so.

The agreement must obligate the business partner to make its internal practices, books, and records relating to the use and disclosure of PHI available to HHS for purposes of determining the covered entity's compliance with the privacy regulations.<sup>19</sup> Again, the covered entity may consider closely paraphrasing the language in the regulation for this provision. Business partners, 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 must also stipulate that upon termination, the business partner will return or destroy all PHI received from the covered entity and will not retain copies of such information.<sup>20, 21</sup>

While not expressly required by the proposed regulations, the agreement should also state that if the business partner chooses to destroy the PHI, it will certify to the covered entity that it has done so. Since the business partner will perform this function after termination of the agreement, there should be language that states that the provision requiring return or destruction of PHI upon termination of the agreement would survive such termination. Otherwise, the business partners' obligation to do so arguably ends upon termination of the agreement.

When a request to correct PHI is accepted by the covered entity, the entity must make reasonable efforts to notify other entities, including business partners, of the correction.<sup>22</sup> The business partner agreement must obligate the business partner to incorporate any corrections to PHI when notified of such correction by the covered entity.<sup>23</sup>

Again, the covered entity may choose to paraphrase the language in the regulation itself for this provision in the agreement. Business partners may try to get this obligation qualified or restricted. The regulation does not appear to anticipate restrictions or qualifications to the business partner's obligation to correct PHI, once informed of such correction by the covered entity.

### **HIPAA contract compliance flow sheet**

Type of contract	Have	Copy received	To legal	OK
Agents/contractors accessing personally identifiable health information				
Coding vendor contracts				
Computer hardware contracts				
Computer software contracts				
Data warehouse/clearinghouse vendor contracts				

Emergency services contracts				
Employment contracts				
Hospitalist contracts				
Insurance contracts				
Legal services contracts				
Microfilming vendors				
Optical disk conversion vendors				
Pathology service contracts				
Paper recycling contracts				
Payer contracts				
Physician contracts				
Professional services contracts				
Radiology service contracts				
Record copying service vendors				
Release of information vendor contracts				
Revenue enhancement vendors				
Risk management consulting vendors				
Shared service/joint venture contracts with other healthcare organizations				
Telemedicine program contracts				
Temporary staffing agencies (when staff have access to health information)				
Transcription vendors				
Waste hauling/incineration contracts (if protected health information is involved)				

Finally, the covered entity must be able to terminate the contract if the covered entity determines that the business partner has violated a material term of the contract.<sup>24</sup> Here, the covered entity will almost assuredly want more specificity than that stated in the regulations. The covered entity 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 covered entity need not provide a cure period

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

**In Addition: Suggested Provisions**

In addition to the required provisions discussed above, there are several additional provisions that covered entities should consider including in business partner agreements. There may be additional provisions not discussed here that the covered entity may want to include in its business partner agreements.

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

Under the proposed regulations, covered entities must issue a notice of information practices.<sup>25</sup> Business partners are bound by the information practices of the covered entity with whom they contract.<sup>26</sup> Covered entities should consider including a provision in their business partner agreements to that effect.

Business partner agreements should give the covered entity the right to audit and monitor the business partner to confirm compliance with the agreement and privacy regulations. (This is in addition to the required provision that allows HHS to audit the business partner.)

**a contracts checklist**

This is a sample list only and may not contain all of the provisions necessary for an effective business partner agreement that complies with HIPAA.

Completed

Completed	Requirements
	Contractor to limit access to PHI based on need to know
	Contractor cannot use PHI in a way that would be violation of regulations if done by covered entity
	Contractor can use PHI only as permitted under the agreement
	Contractor must protect the integrity and availability of data/information
	Standard confidentiality provisions <ul style="list-style-type: none"> <li>• contractor can make no further dissemination without approval</li> <li>• contractor will implement and maintain appropriate safeguards to prevent inappropriate use or release</li> <li>• contractor will inform of breach and cooperate in mitigation</li> <li>• contractor will return/destroy PHI at termination</li> <li>• contractor will retain no copies</li> </ul>
	Contractor will make PHI available as if a covered entity
	Contractor must comply with applicable provisions of regulations
	Contractor will make internal practices, books, and records available to HHS
	Contractor will incorporate corrections to PHI
	Termination for: <ul style="list-style-type: none"> <li>• material breach</li> <li>• repeated non-material breac</li> </ul>
	Individuals about whom information pertains are third-party beneficiaries

	Contractor bound by covered entity's notice of information practices
	Covered entity can audit contractor to confirm and monitor compliance
	Revision based on change to law/regulations
	Compliance with transaction standards (if business associate)
	Amend agreement as HIPAA regulations are modified
	All of above provisions flow down to subcontractors
	Injunction not exclusive remedy
	Indemnification

Business partners may try to limit covered entity audits to a specified number per year and may resist ongoing monitoring. However, covered entities would allow such restrictions at their peril. A material breach by a business partner of any of the provisions required by the regulations will be considered to be noncompliance by the covered entity itself if the covered entity knew or reasonably should have known of such breach and failed to take reasonable steps to repair the breach or terminate the agreement.[27](#)

Some people believe that the regulation imposes a duty on covered entities to monitor their business partners' adherence to the regulations. Arguably, the wording of the regulation does not impose such a requirement. HHS has stated that there is no duty to monitor a business partner's performance unless the covered entity knew or should have known of improper use of PHI by the business partner.[28](#)

Therefore, covered entities need the contractual right to audit and monitor the business partner. HHS will be modifying and adding to the HIPAA regulations. Consequently, any agreements with business partners should, at a minimum, require the business partner to negotiate amendments to the agreement in good faith to accommodate such changes. However, promises to negotiate are rarely worth much, because parties can negotiate but never reach agreement. Consequently, covered entities should seek language that would automatically require the business partner to satisfy any changes in the regulations that the covered entity itself must satisfy. Business partners are likely to rigorously resist inclusion of such language in the agreement because of the open-ended and unknown nature of the obligations.

The covered entity must anticipate breaches of the agreement by business partners and will want to be able to obtain an injunction to stop any continuing breach. Therefore, the covered entity will want a provision allowing it to seek an injunction as well as damages. The provision should state that the covered entity 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 covered entity to be in violation of the regulations if its business partner is in violation, an entity should require very strong indemnification and "hold harmless" language in the agreement. This language should require a business partner to pay defense costs and any expenses that the entity suffers as a result of a breach of the agreement by the business partner, its employees, agents, or subcontractors. This provision should allow the covered entity to control its own defense and make settlements and should protect the covered entity's officers, employees, and agents, in addition to the covered entity itself.

However, indemnification provisions are only as good as the financial resources available to the person who is giving the indemnification. Therefore, in addition to indemnification, the covered entity should consider requiring the business partner to post a fidelity bond to cover the possibility that its employees will misuse the PHI.

Additionally, the covered entity could require the business partner to have certain minimal levels of insurance that would cover inadvertent violation of the regulations and name the covered entity as an "additional insured" on such policies. The agreement should require the business partner to produce a

certificate from the insurance company showing that the covered entity is in fact an "additional insured." The covered entity might even consider reviewing the policy to ensure that exposure under HIPAA is covered. Keep in mind, however, that hardware or software is merely a tool to be used by covered entities to assist them in becoming HIPAA compliant.

Finally, if the covered entity 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. Covered entities 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.

If the agreement states that the vendor will provide upgrades to its product for free, what will happen if the vendor decides not to do an upgrade to an existing product, but produces an entirely new product altogether? The covered entity would be left with a software product that does not comply with revised regulations and no contractual obligation on the part of the vendor to do anything about it. In such a scenario, the vendor may charge significant amounts of money from the covered entity for either a customized product or purchase of the new product that it is marketing. "A Contracts Checklist," page 49, lists the provisions discussed above.

### **Start Preparing Now**

The HIPAA regulations will have dramatic effects on covered entities, not least of which is the effect on business partner agreements. Several provisions discussed above will be required in these agreements. Additionally, other provisions are called for to protect covered entities. Many agreements currently in place will need to be amended, and a tremendous amount of work will need to be done to satisfy all of the regulations.

Covered entities should begin now to inventory their agreements, draft model language, develop a work plan to negotiate amendments to existing agreements as necessary, and develop exit strategies that may need to be implemented in the event negotiations for amendments are not productive.

Understanding the need for such activities will help HIM professionals enhance their knowledge of HIPAA and assist them in bringing their facilities to compliance.

---

### **Notes**

1. "Health Insurance Portability And Accountability Act Of 1996." Public Law 104-191. August 21, 1996. Available at <http://www.access.gpo.gov/>.
2. These provisions were codified at 42 USC §1320d through 1320d-8.
3. Public Law 104-191, 110 stat. 2066, §264 (c) (1996).
4. "Notice of Proposed Rule Making for Standards for Privacy of Individually Identifiable Health Information." Federal Register 64, pp. 59,918-60,064 (November 3, 1999).
5. Proposed regulation 45 CFR §160.102 and 164.502.
6. Proposed regulations 45 CFR §163.103 and §164.504, Federal Register 64, pp. 60,050 and 60,053 (1999).
7. Ibid.
8. Proposed regulation 45 CFR §164.524, 64 Federal Register 60,064 (1999).
9. Ibid.
10. Proposed regulation 45 CFR §164.506, 64 Federal Register 60,054 (1999).
11. Ibid.
12. Ibid.
13. Proposed regulation 45 CFR §164.506, 64 Federal Register 60,054 through 60,055 (1999).
14. Ibid., p. 60,054.
15. Ibid.
16. Ibid, p. 60,055.
17. Ibid.

18. Ibid.
  19. Ibid.
  20. Ibid.
  21. Ibid.
  22. Proposed regulation 45 CFR §164.516(c)(3)(iii), 64 Federal Register 60,061 (1999).
  23. Ibid.
  24. Ibid.
  25. Proposed regulation 45 CFR §164.512, 64 Federal Register 60,059 (1999).
  26. 64 Federal Register 59976 (1999).
  27. Proposed regulation 45 CFR §506(e)(2)(iii), 64 Federal Register 60,055 (1999).
  28. 64 Federal Register 59,950 and 59,991 (1999).
- 

### **FORE announces 2000 grant recipients, 2001 research priorities**

The Foundation of Research and Education (FORE) has presented two grants for studies furthering HIM goals. Karen A. Wager, DBA, RHIA, and Andrea W. White, PhD, RHIA, of the Medical University of South Carolina, have received a grant from FORE for their proposal "The Impact of Direct Entry into the EMR on the Physician-Patient Relationship." This study will determine whether direct entry into the EMR alters physician-patient relationships within an adult primary care center as perceived by patients.

Valerie Watzlaf, PhD, RHIA, and Patricia Firouzan, MSIS, RHIA, of the University of Pittsburgh, have received a grant from FORE for their proposal "Standards for the Content of Electronic Health Records." This study will measure the minimum content recommended in the ASTM E1384 Standard Guide on Content and Structure of Electronic Health Records and corresponding ASTM E1633 Coded Values for Electronic Health Records.

Grant-In-Aid Awards fund studies that are pivotal to the profession's leadership role in health informatics research and its application to healthcare policy and practice, as well as to the vitality, visibility, and viability of the profession and the HIM professional. Dissertation Assistance Awards are also available to fund dissertation research in these areas.

2001 research priorities focus on topics relating to privacy, data quality, and work force issues.

Submissions that address one or more of these issues will receive priority for consideration for funding through the FORE Grant-In-Aid and Dissertation Assistance programs. Priority will also be given to proposed research that is directed toward achieving one or more of the following outcomes:

- policy development
- documentation of current status
- standards development establishment
- validation of a theory
- obtaining benchmark data
- validating best practice
- improving current practice

A more detailed listing of the 2001 research priorities and applications for 2001 Grant-In-Aid and Dissertation Assistance Awards are available at [www.ahima.org](http://www.ahima.org) or by e-mailing [fore@ahima.org](mailto:fore@ahima.org). **The deadline for submissions is May 1, 2001.**

---

*Michael C. Roach is an attorney with Bell, Boyd & Lloyd LLC, based in Chicago. He can be reached at [mroach@bellboyd.com](mailto:mroach@bellboyd.com) or (312) 807-4354.*