

HIPAA BUSINESS ASSOCIATES — BE AWARE OF CONTRACTING RESPONSIBILITIES AND WARY OF RISKS

By Jeanine Freeman, JD

The HIPAA Privacy Rule requires physicians who are HIPAA covered entities to assure through contract the cooperation of their business associates in meeting the physician's use and disclosure obligations under the rule. In doing so, medical practices must pay close attention to contract language to meet their HIPAA responsibilities while avoiding unintended legal liability for contract violations of their business associates.

The business associates rule - its basics. A physician who is a HIPAA covered entity may disclose protected health information (PHI) to a business associate and may allow a business associate to create or receive PHI on its behalf if the physician obtains satisfactory assurance that the business associate will appropriately safeguard the PHI. "Satisfactory assurance" must be documented in a written contract with the business associate and must satisfy the requirements of the Privacy Rule.

HIPAA regulates the relationship that physicians have with their business associates; HIPAA does *not* regulate the business associate. Investigations by the Office of Civil Rights (OCR) will focus on physician compliance with the Privacy Rule.

Who is a business associate? The Privacy Rule includes as business associates those persons who on behalf of a physician assist in the performance of: 1) functions or activities involving use or disclosure of PHI, including claims processing, data analysis, utilization review/quality assurance, billing, benefit management or any other function regulated under HIPAA or 2) support services such as legal, actuarial, accounting, consulting, data aggregation, management, accreditation, and financial services involving the disclosure of PHI.



Jeanine Freeman is vice president of legal affairs for the Iowa Medical Society.

Members of a physician's workforce (employees, volunteers, and others under the direct control of the physician) are not business associates nor are those persons who perform functions for the physician's practice as part of an organized health care arrangement (OCRA). *Caveat:* Volunteers who work off-site and who use PHI to perform their functions are considered business associates.

Disclosure by a covered entity to a health care provider for treatment purposes does not give rise to a business associate relationship nor does disclosure of PHI by a physician to a health plan for payment purposes. Physicians are not required to enter into business associate contracts with hospitals where they have clinical privileges.

Do I need a business associate contract with a person that performs services for me that ordinarily do not call for use or disclosure of PHI? No. Even in cases of incidental disclosure of PHI (i.e., janitorial services, electrician, repairmen), a business associate contract is not required so long as the incidental use/disclosure is limited in nature, occurs as a byproduct of duties being performed, and could not be reasonably prevented. Similarly, entities that act merely as conduits for PHI (i.e., post office, private couriers/electronic equivalents) are not business associates; a conduit transports PHI but does not access it other than on a random basis as necessary to carry out its functions.

The business associates rule - its timing. The Privacy Rule has a "transition period," giving physicians more time to amend EXISTING contracts. A contract is "existing" if in writing prior to October 14, 2002 and not amended or renewed by the parties prior to the Privacy Rule's compliance date of April 14, 2003.

RESOURCES

HIPAA Privacy Rule <http://www.hhs.gov/ocr/combinedregtext.pdf>.

Definition of a "business associate": Rule 160.103

Standard on "satisfactory assurances": Rule 164.502(e)

Standard on "contract requirements": Rule 164.504(e)

Standard on "mitigation" if business associate violates contract terms: Rule 164.530(f)

Compliance deadline/transition period: Rule 164.532 (d), (e)

Sample OCR language: <http://www.hhs.gov/ocr/hipaa/contractprov.html>

OCR guidance statement (12/3/02): <http://www.hhs.gov/ocr/hipaa/privacy.html> (includes helpful discussion on the business associate rule).

Physicians can continue to operate under existing contracts without business associate language until April 14, 2004 or until the contract is renewed or modified, whichever occurs first. Existing "evergreen" (automatic renewal) contracts need not be amended until April 14, 2004 unless the contracting parties otherwise open up negotiations or amend terms. Contracts entered into and signed after October 14, 2002 must include business associate privacy practices contract language by the HIPAA compliance date of April 14, 2003. For those business associates with whom the physician now has an oral agreement, the physician must have written business associate contract language in place by April 14, 2003.

Bear in mind: The transition period for existing contracts does not alleviate the physician from all HIPAA obligations relative to those business associates. Effective April 14, 2003, the physician must provide individuals access to their PHI even if that PHI is held by a business associate; must be able to amend PHI held by the business associate if the physician determines a requested amendment is appropriate; and must be able to receive an accounting of disclosures of PHI made by the business associate. The physician also must mitigate known inappropriate uses of PHI by a business associate consistent with the Privacy Rule and must cooperate with the OCR in any compliance matter, including accessing PHI held by a business associate.

Do I have to monitor my business associates' behaviors? The OCR clarified that the Privacy Rule does not require a physician to actively monitor the actions of its business associates. If, however, a physician knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate contract, the physician is required, to the extent practicable, to take steps to cure the breach or end the violation, including termination of the contract.

Suppose I know of a violation of a privacy practice by my business associate but I need the contracting relationship anyway? So long as a physician has complied with the mitigation steps, the physician may not be required to terminate the contract if such termination is not practicable (i.e., other service options not available), in which case the physician must notify the OCR.

Is there model language I can use? The Privacy Rule sets forth key provisions that must be a part of a business associate contract and gives model language that can get physicians started. Visit <http://www.hhs.gov/ocr/hipaa/contractprov.html>. That model language, however, is NOT a regulatory safe harbor, arguably goes beyond the requirements of the Privacy Rule, and does not necessarily protect physicians against liabilities that might accrue to them for non-compliant privacy acts or practices of their business associates. Model language also has been developed by the Illinois State Medical Society (ISMS) in its policies and procedures manual, now being adapted by IMS with permission of ISMS for IMS member use. Check for this manual on the IMS web site at www.iowamedical.org. WEDI SNIP's "Privacy Policies and Procedures: A Resource Document" sets out provisions that need to be in a business associate contract. You can find this document at http://snip.wedi.org/public/articles/Privacy_PP1115_02.pdf. IMS will notify members of other sources when identified through the IMS web site.

Should I involve my attorney? Yes, it is advisable to involve legal counsel because of potential contractual liabilities. In addition, your attorney may need to assist in negotiations with difficult business associates.