



April 6, 2010

"TIPS" Newsletter  
HIPAA Privacy Series FAQ's 4th in Series



By Edie Hofmann (Edie Ruark Dahlhauser), President ICCOM, LLC  
[edie@ICCOM.org](mailto:edie@ICCOM.org)

You need to know about HIPAA Privacy and Security. This is the third in a series of FAQ's about HIPAA Privacy and Security to help you understand your responsibilities under the HIPAA Rules. Are you HIPAA compliant?

The full HIPAA Privacy and HIPAA Security Compliance Checklists are available on our website:

[HIPAA Privacy Checklist](#)  
[HIPAA Security Checklist](#)

---

HIPAA Privacy and Security, FAQ's  
.....Continued

[Business Associate Agreements](#)

[What is the intent of business associate agreements?](#)

One of the purposes of HIPAA again is to safeguard protected health information (PHI). To the extent you have control of protected health information, you must take appropriate steps to accomplish this security. In a health care practice, many of the provisions of this rule apply to "business associates" who have contact with you and, therefore, access to PHI.

You cannot release or disclose PHI to business associates unless both parties have a business associate agreement in place. The business associate agreement must contain a confidentiality clause that holds the business associate accountable for protecting private PHI. The business associate cannot use or further disclose the information in any way that violates the Privacy Rule.

When a relationship with a business associate ends, the business associate must return or destroy all PHI within a reasonable time frame.

[Who qualifies as a business associate?](#)

A business associate is any person with whom the practice discloses protected health information (PHI) for the purpose of carrying out, assisting in the performance of, and performing for or on behalf of, a function or activity for the practice. This includes persons or contractors who receive PHI from your practice in the course of providing a service to you. You may only disclose this confidential PHI to a business associate if the associate has taken steps to ensure the confidentiality of the information.

#### What types of functions do business associates typically perform?

Functions or activities typically performed that involve the use or disclosure of individually identifiable health information include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and reprising.

#### Who doesn't qualify as a business associate?

The following do not qualify as business associates under the Privacy Rule.

- A. Employees.
- B. Contracted employees who perform a substantial portion of their work at your practice, such as a physical therapist.
- C. Some government oversight agencies.
- D. Hospitals, unless the hospital performs billing services for staff providers.

#### What about when information is shared for treatment purposes?

Any practice or provider may share protected health information (PHI) with a health care provider for treatment purposes without a business associate agreement so long as information is used to treat the patient and not for other unrelated usage.

#### Do I need a business associate agreement for my cleaning service?

You are not required to enter into a business associate agreement with your janitorial service because the performance of such service does not involve the use or disclosure of protected health information (PHI). In most cases, a janitor has incidental contact and such disclosure is permissible as long as reasonable safeguards are in place. It would be ideal to lock the records room or store records in lockable cabinets.

#### Since I already have an attorney-client relationship with counsel, do I need a business associate agreement?

While the Privacy Rule does not intend to interfere with this relationship and feels access to privileged protected health information (PHI) is limited, it does believe that it is appropriate to have attorneys sign a business associate agreement.

### What about organizations that act merely as a conduit of protected health information (PHI)?

The rule does not require a business associate agreement with a person or organization that acts merely as a conduit of information, such as the U.S. Postal Service, certain private couriers, and their electronic equivalents. Since no disclosure is intended and the probability is small for incidental release, no agreement is necessary.

Neither are financial institutions considered business associates when it processes consumer-conducted financial transactions by debit, credit, or other payment cards, checks, or electronic funds transfers. Covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements.

### PHI Return or Destruction

#### What is the requirement for the return or destruction of protected health information (PHI)?

The Privacy Rule requires the return or destruction of all PHI at the termination of a contract only where feasible or permitted by law. When return or destruction is not feasible, the contract must state that the information will remain protected as long as maintained and any further use of this information will be limited to those purposes that make return or destruction infeasible.

Destruction of records in your possession should include cross shredding. You can purchase those shredders at your local office supply store.

### Staff Training

#### What are the requirements for training my staff and who needs to be trained?

There are no set standards for training in the federal regulations except that all staff, including professional staff such as doctors, must be trained initially and annually about HIPAA privacy. This training must take place before (effective date). All new employees must receive HIPAA training as part of their initial orientation to your practice.

Privacy is very important in health care and training your staff to understand the regulations can help to avoid accidental disclosures of information and privacy complaints from patients. Annual privacy training is strongly advised for your practice.

Everyone that handles protected health information (PHI) should be trained in the HIPAA regulations. Everyone who works in your office should be trained about confidentiality.

#### What does my staff need to know about HIPAA?

They should understand the patient rights listed in the Notice of Privacy Practices (NPP) and how to handle any questions or requests by a patient. Having good policies and procedures in place, and having your staff familiar with them, is the best place to start. A HIPAA privacy

training agenda is provided below to assure that the basic information is covered. This may be modified to suit your practice needs. All doctors, staff, employees, and contract personnel should sign a confidentiality agreement.

Everyone in your office should be trained about patient confidentiality including your cleaning service and maintenance people.

### **How do I prove training took place?**

Use a sign-in sheet, keep an agenda of issues covered, and document your staff's training in their employment records. The best way is to test your staff with a written test. Use the written test and test key in this manual for better documentation of your staff training. Issue each staff person a certification upon successful testing.

### **You should retain HIPAA training records for six (6) years.**

#### **State Verses Federal Law**

HIPAA requires that you know, understand and follow your state law. You are required to be compliant with whichever is more stringent.

To be continued...(Specific HIPAA Security FAQ's will begin)

(to be continued)

=====

**Please visit my website that further explains the HIPAA rules and more about the compliance manuals available.**

**[http://www.iccom.org/index\\_files/ICCOMProducts.html](http://www.iccom.org/index_files/ICCOMProducts.html)**

**email me with any questions you may have: [edie@iccom.org](mailto:edie@iccom.org)**

**If you no longer wish to receive these helpful "TIPS", please unsubscribe by using "Manage your subscription" below. Thank you.**