

HIPAA Training Handbook for Rehab Providers

*An Introduction to Confidentiality
and Privacy Under HIPAA*



HIPAA Training Handbook for Rehab Providers: An Introduction to Confidentiality and Privacy Under HIPAA is published by HCPro.

Copyright 2003 HCPro

All rights reserved. Printed in the United States of America.

ISBN 1-57839-248-9

No part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro or the Copyright Clearance Center (978/750-8400). Please notify us immediately if you have received an unauthorized copy.

HCPro provides information resources for the health care industry. A selected listing of other products is found in the back of this book.

HCPro is not affiliated in any way with the Joint Commission on Accreditation of Healthcare Organizations, which owns the JCAHO trademark.

Betsy Anderson, BS, and Terry Cichon, CPA, Authors
Christine Hannan, Senior Managing Editor
Jean St. Pierre, Creative Director
Mike Mirabello, Senior Graphic Artist
Tom Philbrook, Cover Designer
Kelly Wallask, Group Publisher
Suzanne Perney, Publisher

Advice given is general. Readers should consult professional counsel for specific legal, ethical, or clinical questions.

Arrangements can be made for quantity discounts.

For more information, contact:

HCPro
P.O. Box 1168
Marblehead, MA 01945
Telephone: 800/650-6787 or 781/639-1872
Fax: 781/639-2982
E-mail: customerservice@hcpro.com

**Visit HCPro at its World Wide Web sites:
www.hcmarketplace.com, www.hcpro.com, www.hcprofessor.com,
www.rehabregs.com, and www.himinfo.com.**

Contents

About the experts	vi
Intended audience	1
Part 1: Overview	1
What is HIPAA?	1
Parts of HIPAA may sound familiar	3
Are we a covered entity?	3
HIPAA gives patients new rights	5
What kind of information is protected?	6
Part 2: Administrative requirements	7
Key people under HIPAA	7
All staff must be trained	7
Protecting patients' privacy	7
What if we break a HIPAA rule?	8
Put HIPAA compliance down on paper	9
Part 3: Penalties for noncompliance	10
Strict penalties for ignoring the rules	10
Part 4: The Notice of Privacy Practices	11
Case study #1: Patient expectations	11

Part 5: The minimum necessary standard	11
What do I need to know?	11
Part 6: Some conversations should be private	12
How do I know what's appropriate?	12
Case study #2: Loose lips	13
Case study #3: Gender bender	15
Part 7: Handle PHI carefully	16
Case study #4: Finders keepers	16
Watch where the PHI ends up	17
Case study #5: Teenage pranks	19
Part 8: Safeguard computers	20
Protect the machines	20
Protect PHI in computers	20
Part 9: Incidental v. accidental disclosures	21
Sometimes it can't be helped	21
To fax or not to fax?	22
Part 10: Patient authorizations	24
When do I need an authorization?	24
One alternative to authorizations	25

Part 11: Business associates	25
Are you a business associate, or do you have any?	25
Who are your business associates?	26
Two exceptions to the rule	27
Part 12: Marketing under HIPAA	28
Know what kinds of marketing you do	28
Get permission from the patient	28
Part 13: Fundraising and HIPAA	29
Do I need an authorization?	29
Part 14: HIPAA, your finances, and patient care	30
The bottom line	30
Caring for patients under HIPAA	31
Final exam	32
Answers to final exam	36
Related products	37
Certificate of completion	40

About the experts

Betsy Anderson, BS

Betsy Anderson, BS, is vice president of FR&R Healthcare Consulting, Inc., in Deerfield, IL. She joined FR&R in 1989 and has been instrumental in the development of FR&R's expertise in the health care industry. She specializes in reimbursement, regulatory, and operational consulting. Previously, Anderson was a Medicare auditor at a fiscal intermediary in Illinois.

Anderson provides educational seminars on a wide variety of topics including HIPAA, Medicare and the prospective payment system (PPS), billing and accounts receivable, Medicaid, and regulatory issues. She works with various providers including rehabilitation, long-term care, assisted living, and senior housing. Anderson is a graduate of Northern Illinois University in DeKalb, IL, where she received her bachelor's of science degree in accountancy. Anderson also studied nursing education for three years at Aurora University in Aurora, IL.

Terry Cichon, CPA

Terry Cichon, CPA, is director of health care operations at FR&R Healthcare Consulting, Inc. She joined FR&R in 1996 and specializes in reimbursement, operational, and management consulting. Prior to joining FR&R, Cichon was the president and chief financial officer of a rehabilitation organization that provided staffing, durable medical equipment, and outpatient clinic services.

Cichon has provided educational seminars on management, data analysis, billing, budgeting, PPS, HIPAA, compliance planning, and business development. She has also written articles for compliance and home health professional journals. She works with rehabilitation, home health, hospice, physician practices, and long-term care providers. Cichon received her bachelor's degree in management from Lewis University in Romeoville, IL.

About FR&R

FR&R Healthcare Consulting, Inc., provides consulting services to the health care industry on regulatory, reimbursement, and management issues. The health care practice of FR&R offers services to therapy groups, physician practices, the long-term care industry, home health providers, assisted living facilities, and hospice organizations. FR&R's health care specialists have experience with all regulatory and reimbursement issues including HIPAA and corporate compliance planning, strategic planning, interim chief financial officer services, financial management, budgeting, and cost control analysis. In addition, the firm assists its clients with Medicare and Medicaid audits, Office of Inspector General investigations, nursing chart reviews, staffing issues, and MDS and OASIS completion.

FR&R Healthcare Consulting, Inc.
111 Pfingsten Road Suite 300
Deerfield, IL 60015
847/236-1111 (phone)
847/236-1155 (fax)

www.fronline.com

SAMPLE

©2003 HCPro, Inc. Unauthorized duplication is prohibited.

HIPAA Training Handbook for Rehab Providers

An Introduction to Confidentiality and Privacy Under HIPAA

Intended audience

- Physical therapists
- Physical therapist assistants
- Occupational therapists
- Certified occupational therapist assistants
- Speech pathologists
- Therapy aides
- Administrative staff
- Office and practice managers

Part 1: Overview

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains three major regulations that affect health care providers:

- Standards for electronic transactions
- Security standards
- Standards for privacy of individually identifiable health information

Electronic transactions standards. This portion of the regulation addresses the requirement that all covered entities use uniform coding standards when processing certain designated transactions in electronic format. The original compliance date was October 16, 2002, but covered entities that filed a compliance plan were granted an extension. Covered entities now must begin testing their electronic systems by April 16, 2003, and must be fully compliant by October 16, 2003.

Security standards. This portion of the regulation addresses the integrity, confidentiality, and availability of electronic data in a covered entity. The final rule for this regulation was published February 20, 2003. The compliance date will be 24 months after the publication of the final rule, or April 21, 2005.

Privacy of individually identifiable health information.

Commonly referred to as the privacy rule, this section of the regulation addresses patients' rights and the duty of the covered entity to protect the privacy of patients' medical information. The compliance date for this portion of the regulations is April 14, 2003.

This handbook provides a basic understanding of the HIPAA privacy rule and how it affects the delivery and payment of care. Like all health care providers, physical, occupational, and speech therapists will need to make some changes in the way they use and disclose patient information. It's crucial that you can differentiate between the myths and realities of the privacy rule and understand its effect on day-to-day operations.

Parts of HIPAA may sound familiar

The privacy rule requires that we ensure the privacy of certain information about patients in any form—oral, written, or electronic. The good news is that most health care organizations, including therapy providers, have done an excellent job in the past of ensuring that they have not inappropriately disclosed written and electronic health information to anyone outside of the organization. Usually, all requests for medical records are reviewed and processed in accordance with the organization's policies and procedures.

Are we a covered entity?

One of the first tasks that rehabilitation providers face is defining whether they are a covered entity (meaning they must comply with HIPAA) and, if so, what type of covered entity they are. While this is a task usually reserved for managers and their lawyers, understanding the various types of covered entities will help staff recognize the communication barriers that can exist between covered entities. Rehab companies may be any of these four types of entities:

- **Single covered entity.** This can be as small as a physical therapist in independent practice or as large as a major health system. It could have covered entities, such as a hospital, and noncovered entities, such as an independent living facility. If it is one legal entity, the important thing to understand is that all elements of this single covered entity can communicate with each other regarding patient treatment, payment, and health care operations.

- **Affiliated entities.** These are separate legal entities that share common ownership or control. They could be a nursing home, therapy company, and home health agency that share at least 5% common ownership or control. These entities may choose to be individual covered entities or may designate themselves as affiliated. Being affiliated means they can share information and even share some of the required tasks of a covered entity.
- **Hybrid entity.** This is an organization that has a health care component but whose major business is not providing health care. An example of a hybrid organization is a therapy clinic established at a major manufacturing plant to provide rehabilitation to its workers who are injured on the job. As a hybrid, all of the non-health care components are exempt from the privacy regulations. However, this means that the health care component cannot communicate health information freely with the rest of the organization.
- **Organized health care arrangement (OHCA).** This exists when unrelated covered entities provide health care in a clinically integrated setting or when unrelated covered entities participate in an organized system of health care, such as a network of providers. Organizations that operate as an OHCA can share information and some of the required tasks of a covered entity.

HIPAA gives patients new rights

Under HIPAA, patients have five individual rights:

- Right to request privacy protection for protected health information (PHI)
- Right to access PHI
- Right to request an amendment of PHI
- Right to request an accounting of disclosures of PHI
- Right to a copy of the provider's Notice of Privacy Practices

The **right to request privacy protection** means that patients can ask a covered entity to not use or disclose some types of protected health information in certain ways or to certain people such as their family members. The covered entity does not have to agree to this request but, if it does, the organization is required to abide by that restriction. The patient also has the right to request that the organization communicate with them in a certain way or at a certain place. If the request is reasonable, then the organization must agree to these forms of communication.

It is important that all staff members know when one of these requests has been agreed to. If a patient has requested that you not contact him at work and you call there to change an appointment, you have violated the patient's right to privacy. If a patient requests that you not speak with her son about her treatment and you agree, but the son calls and you provide him with information, then you have violated the patient's right to privacy.

The **right to access PHI**, the **right to request an amendment to PHI**, and the **right to request an accounting of disclosures of PHI** belong to all patients. Most therapists will not be involved in the process that allows the patient to access this information.

The final individual right is the **right to request a copy of the Notice of Privacy Practices**. This document spells out all of the patient's rights and the organization's responsibilities. The notice must be provided to all patients at the time of their first treatment on or after April 14, 2003. Therapists and administrative staff should be familiar with this document and know when they may be called upon to provide this document or to direct patients to someone who can assist them. In addition to providing the notice to patients, organizations must post it in a visible location in the therapy department or clinic. (The notice must also be posted on the organization's Web site, if applicable.)



What kind of information is protected?

"Protected health information," or PHI, is a very important HIPAA concept that staff members must understand. Basically, it is any element of health information that identifies a patient or provides a reasonable basis for identifying a patient. This includes not only the demographic information, but any other item or characteristic, such as place of employment.

Part 2: Administrative requirements

Key people under HIPAA

The privacy regulations spell out how a covered entity is supposed to implement the privacy rule, including who is supposed to lead the compliance effort for each organization. Knowing who these people are will help you stay on the right side of the HIPAA law.

Each organization must appoint a **privacy officer** to oversee the development, implementation, and monitoring of the HIPAA privacy plan. This is the individual to whom work force members should go if they have any questions concerning matters of patient privacy. The **contact person** must be designated in the organization's Notice of Privacy Practices. This is the person whom patients can contact with questions about their rights, to exercise their rights, or to file a complaint.

All staff must be trained

Every single member of the organization's work force must receive job-specific training prior to the implementation of the privacy rule on April 14, 2003, or when hired. This means that all therapists, administrative staff, students, and volunteers will be expected to understand how to protect a patient's right to privacy. But it is the organization's job to provide you with necessary training.

Protecting patients' privacy

The organization must establish certain safeguards to address administrative, technical, and physical issues related to making

sure PHI is indeed protected. For example, the organization may develop new policies and procedures/revise job descriptions to provide **administrative safeguards**. Your organization may install automatic logoffs on computers and you may be required to change your passwords more frequently. These are **technical safeguards** to ensure the privacy of PHI.



Physical safeguards address issues such as placing printers, facsimile machines, copiers, and computer terminals in secure locations, as well as locking medical records. Limiting the access visitors and vendors have to patient information is also a critical part of the required physical safeguards.

What if we break a HIPAA rule?

Each organization must establish a process that allows all individuals, including people who are not patients, to file a **complaint** regarding a privacy violation. All staff members should be sensitive to the rights of their patients and others and be able to identify any complaints that are verbalized both formally and informally.

Also, in order to demonstrate its commitment to protecting its patients' privacy, each organization must develop a **sanctions policy** that is uniformly applied whenever the privacy rule has been violated.

If an organization discovers a privacy breach, it must take all reasonable steps to **mitigate**, or minimize, the damage caused by the breach.

All organizations must pledge to not retaliate in any way against anyone who reports a violation, participates in an investigation of a violation, or in any other way exercises his or her rights under this regulation. This **nonretaliation** policy must be stated in the Notice of Privacy Practices.

While an organization does not have to agree to every request that patients make to exercise their rights, the organization cannot ask patients to **waive their right** to make the request. There is a big difference between telling patients that they cannot ask to see their medical information and denying the request for legitimate reasons allowed in the privacy regulation.

Put HIPAA compliance down on paper

A covered entity is required to establish **policies and procedures** to ensure that patients' right to privacy is protected. This may mean modification of some of the existing policies and procedures or the development of entirely new ones that are needed to protect the new rights that a patient has under the privacy regulations.

The organization is required to maintain **documentation** that supports the existence of its HIPAA plan. This includes, for example, the policies and procedures discussed above, documentation of requests to exercise individual rights, and complaints.

Finally, HIPAA requires that organizations **retain patients' records** for six years from the date the record was created or was last in effect.

Part 3: Penalties for noncompliance



The Department of Health and Human Services (HHS) has been very clear that it does not want the implementation of the privacy rule to interfere with patient care or to put any health care provider out of business. What is required is a legitimate, concerted effort to comply with the regulation through the development of the proper policies, procedures, and forms and the training of the work force members.

Human nature being what it is, there are going to be mistakes. If an organization makes a diligent effort to comply, HHS has indicated that it will begin the enforcement process with education of the provider.

Strict penalties for ignoring the rules

However, for those organizations that do not make a legitimate effort to comply, the penalties can be significant. Organizations can face civil penalties for violations that occurred because the organization did not take sufficient steps to protect patient privacy. Those penalties range from \$100 per person per violation to a maximum of \$25,000 per year for a single offense.



Individuals or organizations that knowingly and willfully violate the privacy regulations can face fines of up to \$250,000 and/or prison terms of up to 10 years.

Part 4: The Notice of Privacy Practices

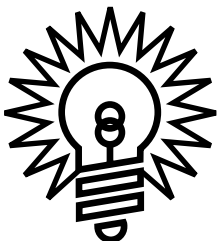
Case study #1: Patient expectations

A potential patient asks to see a copy of your privacy notice, a request allowed under the regulations. She compares your policy to those of other providers and thinks that her medical information is better protected with another provider. She decides to obtain her therapy services from another clinic.

Anyone has the right to request a copy of your privacy notice at any time. You must make sure that *patients* receive a copy of your notice before you provide treatment on or after April 14, 2003. You must also make a “good faith effort” to obtain a written acknowledgement from patients that they have a copy of the privacy notice.

However, you are not required to obtain the written acknowledgement. If the patient refuses to sign the acknowledgement or fails to return it to you, you may still provide services to that patient.

Part 5: The minimum necessary standard



What do I need to know?

The application of the minimum necessary standard will change the way rehabilitation providers conduct their day-to-day operations. This standard is similar to the military’s “need to know” policy. No one in the organization should have access to PHI unless they need it to do their job. If they do need access to PHI, it should be limit-

ed to the “minimum necessary” to allow them to complete their job function.

However, the minimum necessary standard does not apply to therapists or other clinical staff who are providing treatment. They are allowed access to all relevant patient information.

The minimum necessary standard will have the greatest effect on the administrative positions within your organization. In a small organization with one or two administrative employees, there will be very little change in day-to-day operations due to the minimum necessary standard. It is very likely that all employees need access to the information either to do their jobs or as part of their cross training.

However, in a larger organization that has five or more administrative staff members, there likely is enough division of duties to warrant the application of the minimum necessary standard.

Applying this standard may mean that an employee no longer has access to certain records. It will certainly mean that there will be password protection on files that contain PHI, and employees will not be able to share that data.

Part 6: Some conversations should be private

How do I know what's appropriate?

One aspect of the privacy regulations that may require some changes in daily operations is the way that organizations han-

Other oral communications, which are protected by the HIPAA privacy rule. When you're involved in any conversation that contains PHI, consider the following to determine whether the conversation violates the HIPAA privacy rule:

- **Content:** Is PHI being disclosed?
- **Context:** Is this an authorized conversation—does it have a legitimate purpose?
- **Location:** Is there a reasonable expectation that this conversation will not be overheard, or is there no other location in which to have this conversation?

Conversations that do not meet the correct standards for content, context, and location, are probably inappropriate conversations that may be a violation of patients' privacy rights.

Case study #2: Loose lips

Therapist A has contacted a patient at his office after the patient had requested no communication at that location and your organization agreed to that restriction.

Therapist B and one of the office staff were in the lunchroom discussing a patient's idiosyncrasies in the presence of others.

Therapist C created a list of all the patients who use transcutaneous electrical nerve stimulation (TENS) machines to give to her husband, who sells TENS supplies.

What type of discipline is appropriate in each of these cases? The HIPAA privacy rule requires that covered entities establish a process for "sanctioning" members of the work force

when they violate the privacy of a patient, as in each of the examples above.

In the first example, the therapist may not have been aware that the organization agreed to restrict communications at the patient's office. When a covered entity agrees to a request, it must be certain that it can implement the request appropriately. If the therapist was not aware of the agreement, then the organization should not take any disciplinary action. The organization should, however, review its policies and procedures for notifying staff when agreeing to such restrictions from a patient.

In the second example, the oral communication was an inappropriate conversation between the therapist and the office staff member. While PHI was being discussed, it was not in the context of care planning or payment, and the conversation took place where there was no expectation of privacy. Since both the therapist and the office staff member were participating in the conversation, the organization should sanction both of them. If this was their first offense, they should receive reeducation on the basics of the privacy rule. If there were prior offenses, the organization should take disciplinary actions—consistent with existing disciplinary policies.

In the third example, the therapist knowingly and willfully violated the patients' privacy rights. The organization should fire this therapist and could even consider taking legal action against her.

Case study #3: Gender bender

A female patient sits in the waiting room. She is the only female. Her occupational therapist and physical therapist are discussing her condition—lymphedema secondary to her mastectomy. The conversation is within earshot of the waiting area.



How can you prevent others from overhearing the conversation?

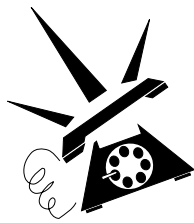


The simplest solution is to avoid having conversations that contain PHI in a location where they can be easily overheard. In the case above, the therapists could have conducted their conversation in a room with a door, to protect the patient's privacy. However, that is not always practical. The following are typical oral communications that take place in a therapy practice that present specific challenges to privacy protection:

- **Clinical discussions.** Clinical staff frequently need to confer to discuss a patient's treatment and progress, or they need to have conversations with the patient. In a clinic or department that does not have a separate office for the clinical staff, these discussions frequently occur in either the reception area or the treatment room. Whenever possible, these discussions should take place away from public locations where they can be easily overheard.

If these conversations must take place in the presence of others, you should make every effort to move to as private an area as possible in the room and you should lower your

voice. If there are curtains in the treatment room, pull the curtains while talking with the patient. Similarly, staff members could go to a treatment area and pull the curtains.



• **Appointment scheduling and confirmation.**

The receptionist is frequently the person who schedules appointments and confirms existing appointments. He or she usually makes these calls at the reception desk within earshot of the waiting room. When possible, the receptionist should make the calls from another room or assign the duties to someone else. If that is not possible, have the receptionist follow these simple steps:

- Close the partitions when not greeting a patient
- If there are no partitions, turn away from the waiting room when handling calls
- Speak in a lower voice
- Avoid mentioning the patient's full name

Part 7: Handle PHI carefully



Case study #4: Finders keepers

A therapist in your practice has completed all of her progress notes on her home computer and brings them to the office on a disk. The therapist leaves the disk in the secretary's inbox. The next day, the disk is missing. A temporary employee found the disk and sold the information to a marketing company.



What should you do to prevent this type of problem?



No one should ever put PHI in someone's inbox. If possible, the therapist should have kept the disk until it could be personally delivered.

However, in a therapy practice that has therapists seeing patients in the field, this is not always practical. The office manager should provide employees who have access to PHI with a key to a file cabinet where PHI can be delivered safely.

No forms of PHI, whether electronic or written, should be left unattended or in areas where anyone can access them. A temporary employee is probably still a member of your work force. Did this employee receive proper education regarding the HIPAA privacy rule? This could be a violation that is punishable by fines and imprisonment.

Watch where the PHI ends up

While much of what you'll need to do to comply with HIPAA is essentially a matter of common sense, there are some common scenarios that can trip you up. Watch out for the following three danger areas:

1. Improper disposal

- A therapist who has written progress notes on his home computer donates the computer to his child's school. Unless the hard drive was "cleaned" with a software program to clear all information, deleted records are still accessible.

- Your office reuses computer diskettes by deleting old files. Anyone who uses an old diskette can access the information that was on the disk unless it has been cleaned.

2. Improper disclosure

- You fax a home health referral to one of your occupational therapists at home. Her son intercepts the fax and recognizes it as the mayor's name. He tells all his friends that his mom is treating the mayor.
- A physical therapy student who is interning in your practice is doing a term paper on the use of electrical stimulation as a treatment modality for wound care. Your office manager gives the student copies of the files and the names of all your patients who have received this treatment in the past year.

3. Improper access

- Your receptionist's son has the day off from school and she couldn't find a babysitter. She brings him to work with her and lets him "play" on the computer. He is able to access patient demographic information because his mom entered the computer with her password.
- The schedule was overloaded today so none of the therapists were able to write their documentation. All of the patient files are left out in the therapy department to remind the therapists to complete their notes

the next day. The first patient in the next morning arrives early and has access to all of the files.

Case study #5: Teenage pranks

The billing manager was behind in making collection calls and decided to make some of the calls from home over the weekend. She brought the records home on a computer disk and loaded them into her computer. She worked Saturday morning and then left to run some errands. Her 17-year-old son had overheard his mother making calls and thought it would be fun to make some calls and tell people they were being sent to a collection agency.



What should you do about children and other family members?



The privacy regulations pose significant challenges to employees who work at home as part of an established arrangement on an occasional basis to catch up with work from the office. All PHI should be maintained in accordance with the privacy regulations at all times. This means that employees should lock up PHI or make it inaccessible in accordance with the minimum necessary standard. Here are some considerations when working from home:

- Safeguard records while transporting them. For example, keep them in a locked briefcase.
- Work at home in a private area without other family members having access to the PHI.
- Never leave PHI unattended in the home.
- Your home computer should have the proper technical safeguards.

Part 8: Safeguard computers



Protect the machines

To safeguard your computers, you need to consider control of both the computer itself and the data that it can access. The physical placement of the computer is an important consideration.

Can patients at the registration desk read information on the computers? You can turn monitors so that patients cannot view them. If that isn't possible, you can purchase polarized screens to make it difficult to read the data from an angle.

Also, make sure your organization monitors the removal of laptops, point of service devices, and other portable electronic equipment. Be sure that only authorized staff are taking these devices out of the office.

Protect PHI in computers

There are two aspects to controlling patient data that's stored in computers: data access and data integrity. To safeguard data access, take the following precautions:

- Use passwords within all software applications
- Control the assignment of passwords and change them frequently
- Install automatic screen logoffs
- Control your software vendor's access to data files

To protect data integrity, take the following steps:

- Restrict use of e-mail to prevent data corruption

through viruses

- Restrict use of unauthorized programs on your computers
- Purchase software programs to establish firewalls and virus protection

Part 9: Incidental v. accidental disclosures

Sometimes it can't be helped

The final privacy rule issued in August 2002 made it clear that the government understands that not all violations are avoidable. For example, it may not always be possible to have a private conversation. Therapists may speak quietly and as far from the waiting room as possible, but are still overheard. Similarly, a therapist discussing care with a patient in the treatment area can pull the curtain, but may still be overheard.

The government has identified these as *incidental disclosures*. An incidental disclosure takes place when the therapy practice has implemented an appropriate HIPAA privacy plan and a disclosure that is otherwise permissible under the regulations is incidentally disclosed to someone who should not have that information.

Another form of incidental disclosure would occur if the copier repair person found a document containing PHI jammed in the copier.

An accidental violation is not the same as an incidental disclosure. An accidental violation is still a violation because

reasonable precautions might have prevented it. These types of violations can frequently occur when faxing PHI.



To fax or not to fax?

HIPAA does not forbid sending or receiving faxes that contain patient information, but there are several issues to consider regarding the use of fax machines.



Where is the fax machine located?



This is an important consideration both when sending and receiving faxes. Newer fax machines have automatic redial capabilities if the number you are calling is busy. This feature encourages the sender to leave the document in the fax machine and let the machine continue redialing at set intervals until the document is transmitted. If you leave unattended a document containing PHI, an accidental violation can occur. Placing fax machines in secure locations can eliminate the risk.

The same is true when receiving a fax. Most people do not call to tell you they are sending a fax and request that you be at the machine to receive it. This would not be practical, considering the number of faxes that most therapy practices receive on a daily basis. Placing the fax machine in a secure location reduces the risk of accidental disclosure if you do not immediately retrieve a fax that contains PHI.



How can I verify that the fax was sent to the correct party?



Again, newer models have both a caller ID window as well as speed dialing. When you preprogram the numbers into the machine, instead of the phone number appearing in the caller ID window, the name of the party that you are sending the fax to will appear.

The government recommends that you use speed dialing to confirm the name of the recipient. At a minimum, you should have a policy that instructs staff to verify the number of the recipient in the caller ID window before transmitting the information. Another level of verification would be to print out the transmission verification page or log.



What should I do when I discover that a fax was sent to the wrong party?



Having a disclaimer on your fax cover sheet is probably not enough. You should be proactive and call the number to which the fax was sent to reinforce that the document was sent in error and request its destruction. But you must go even further. The therapy practice should log this as an unauthorized disclosure and enforce employee sanctions as necessary.



How can I confirm that the person requesting the information has the authority to do so?



First, you should determine the legitimacy of

people making the request. Are they who they say they are? Then, an understanding of what information can be disclosed for treatment, payment, or health care operations is critical. Anything that does not fall under one of the permitted uses or disclosures will require a patient authorization.

Part 10: Patient authorizations



When do I need an authorization?

Therapy providers can use a patient's PHI for treatment, payment, or health care operations within their own practice without an authorization from the patient. You can disclose **treatment information** to another health care provider. You can only disclose **payment information** to another health care provider or another covered entity. You can only make disclosures for the purpose of **health care operations** to another covered entity that has a previously established relationship with the patient.

However, you must obtain **authorizations** for other purposes—especially when you plan to use or disclose PHI for the following activities:

- Marketing in any form
- Fundraising on another organization's behalf
- Any use or disclosure of psychotherapy notes
- Coordination of benefits on fully paid claims

One alternative to authorizations

In rare cases, you may not need to obtain an authorization to use PHI for reasons other than what's normally allowed under HIPAA. One alternative, the **limited data set**, can be used only for research, public health, or health care operations. Therapy providers who participate in research or benchmarking operations may want to consider the possibility of using a limited data set for these activities instead of obtaining necessary authorizations. To qualify as a **limited data set**, certain data elements must be removed.

Once you remove all of these identifiers from PHI, you can use or disclose it without a patient authorization for the limited purposes stated above.

Part 11: Business associates

Are you a business associate, or do you have any?

A business associate is a third party that creates, uses, or discloses PHI when performing a service on behalf of a covered entity. As a therapy provider, you could be a business associate, but you probably also have some business associates if you are a covered entity. Let's look at how your daily operations as a therapy provider would be affected by each of these possibilities.

Some rehabilitation providers may discover that they fit the definition of both a covered entity and a business associate. These organizations usually provide staffing services to other

covered entities, such as skilled nursing facilities or home health agencies, and function as a staffing agency.

When providing services to a skilled nursing facility, therapists frequently must track the procedure codes and amount of time spent with each resident. The therapy company then compiles this information and provides it to the skilled nursing facility in detail to assist them in their billing. These administrative tasks, not the treatment provided, are what makes a therapy company a business associate.

As a business associate of another covered entity, you will be issued a business associate contract to sign. Covered entities must have a business associate contract in place before they can disclose PHI to individuals or organizations that qualify as their business associates.

Business associates are not directly subject to the privacy regulation. It is only through the contract with the covered entity that the business associates have responsibility to ensure the privacy of PHI.

Who are your business associates?

As a covered entity, you have business associates. An individual or business providing the following types of services to your therapy practice is always considered a business associate:

- Accreditation
- Benefit management
- Billing

- Claims processing or administration
- Data analysis, processing, or administration
- Practice management
- Quality assurance
- Repricing
- Utilization review

An individual or business providing the following types of services to your therapy practice is generally considered a business associate, but only if the service involves the creation, use, or disclosure of PHI:

- Accounting
- Actuarial
- Administrative
- Consulting
- Data aggregation
- Financial
- Legal
- Management

Two exceptions to the rule

There are two special cases that affect the designation of a business associate. First, members of your work force do not become business associates based on the services they are providing. A business associate must be a third party.

Second, a third party that only provides treatment is not considered a business associate. In the earlier example of why your therapy practice may be someone else's business associ-

ate, it was not that you were providing treatment for patients that made you a business associate, but rather that you also performed additional administrative tasks on the covered entities behalf. You can use the same test to determine who may be your business associate.

Part 12: Marketing under HIPAA

Know what kinds of marketing you do

The HIPAA privacy regulations require that we be more aware of the many types of marketing that we do and only use the patient's PHI with their authorization. Marketing can be any use or disclosure of PHI within your organization that does not meet the definition of treatment, payment, or health care operations. Letters of praise from satisfied patients that are posted on the bulletin board in a treatment area are really forms of marketing. We want to tell our patients, "Look at us, see how great we are!"

Other forms of marketing are more obvious. It is usually a communication with a patient that encourages him or her to buy a particular product or service. One of the basic tenets of the HIPAA privacy rule is that patients have a right to decide how their PHI will be used.

Get permission from the patient

You'll need to obtain a patient authorization to use or disclose PHI for marketing purposes. And if the therapy practice will receive any type of remuneration for providing that infor-

mation to a third party, you must disclose that on the authorization form.

However, the final privacy rule relaxed some of the restrictions that health care providers felt would have a negative impact on the provision of care and allowed for the following exceptions to the definition of marketing:

- Information about other products or services provided by the therapy practice
- Information about the treatment being provided
- Information about treatment alternatives
- Any face-to-face communications
- Promotional gifts of nominal value

Any materials provided to patients in writing must allow them the opportunity to request that they no longer receive these marketing materials (i.e., the opportunity to “opt out” of future mailings).

Part 13: Fundraising and HIPAA

Do I need an authorization?

The final rule also relaxed the authorization requirements for fundraising. A therapy practice can use its patients’ names, addresses, and dates of service to conduct fundraising on its own behalf without the need for an authorization. Anytime the therapy practice uses any other information from the patient’s PHI, an authorization is required. In addition, you

must obtain an authorization any time you use any of the patient's PHI to conduct fundraising for or on behalf of another organization. Here are two examples:

If your therapy practice is part of a nonprofit health care system, you can send an invitation to patients inviting them to the charity ball being conducted to raise money for the health care system.

If your therapy practice is participating in a 5K run for multiple sclerosis or any other fundraising event not directly connected to the health care system, you could not use patients' PHI, including their names or addresses, to solicit funds unless you obtain an authorization.

Part 14: HIPAA, your finances, and patient care

The bottom line

Every therapy practice must comply with all elements of the HIPAA regulation. However, how each practice does that will be different. For example, in a small, independent physical therapy clinic with one or two therapists and an office manager, there is no need to spend time applying the minimum necessary standard. Everyone needs access to the patient's PHI.

On the other hand, large clinics with 20–30 therapists and five or more administrative staff will need to examine the minimum necessary standard as it affects the administrative staff.

Likewise, training and all other HIPAA requirements will vary in intensity based on the size of your practice. You will definitely have to invest time and resources in your HIPAA compliance efforts, no matter what your size. Determine which is your more precious commodity—dollars or time. The more you can accomplish independently, the less money your practice will spend on outside assistance. The implementation of the HIPAA regulation should not be so onerous as to jeopardize the financial health of your therapy practice.

Caring for patients under HIPAA

However, another important consideration is the effect that the implementation of HIPAA will have on your delivery of patient care. It is not acceptable to refuse to change because it might be difficult to learn new behaviors. However, those new behaviors should not have a negative impact on your ability to render appropriate care and treatment to your patients. If the changes you contemplate would have a significant negative effect on that ability, you may want to revisit some of those changes.

Final exam

- 1. Organizations will automatically have to pay expensive fines if they violate a HIPAA regulation.**

True or False?

- 2. What must covered entities do before April 14, 2003, to comply with the HIPAA privacy regulations?**

- a. Complete written policies and procedures
- b. Train employees on their responsibilities under the law
- c. Both a and b
- d. None of the above

- 3. The HIPAA privacy rule addresses electronic signature standards.**

True or False?

- 4. Knowingly and willfully violating the privacy regulations carries with it which of the following penalties?**

- a. Fine of up to \$250,000 and/or prison term of up to 10 years
- b. Fine of up to \$100,000 and/or prison term of up to one year
- c. Fine of up to \$500,000 and/or prison term of up to five years
- d. Fine of up to \$25,000 and prison term of up to one year

- 5. A therapist is talking to her husband on her cell phone. The therapist tells him that she will be late—she has to see one more patient, a young man who is a motorcycle accident victim. This is a violation of the privacy rule.**

True or False?

6. There are certain activities that therapy practices should complete to be prepared for the HIPAA privacy deadline. What is the first priority?

- a. Work with legal counsel to amend business associate contracts to protect patient information once it leaves your facility
- b. Buy new computers
- c. Work with legal counsel to determine whether you are a covered entity
- d. Review your privacy and confidentiality policies

7. Keeping an appointment list in a file folder at the registration desk is a violation of the HIPAA privacy rule.

True or False?

8. The security rule compliance date is also April 14, 2003.

True or False?

9. How can you ensure the privacy of faxes?

- a. Put the machine in an enclosed area where only authorized personnel have access
- b. Program fax numbers
- c. Call patients first to see whether they authorized someone to see their medical records via fax
- d. All of the above

10. Which of the following documents must a business associate sign?

- a. Business associate authorization
- b. Business associate contract
- c. Business associate notice
- d. Business associate data set

11. Written authorization is required to disclose information to the patient's primary physician.

True or False?

12. Which of these does not require individual authorization before the information can be used or disclosed?

- a. Marketing of non-health items and services
- b. Sale, rent, or barter
- c. Employment determinations
- d. None of the above

13. "Minimum necessary" under HIPAA's privacy rule is the least amount of information people need to know about patients in order to do their jobs.

True or False?

14. Organized health care arrangements do not have to comply with HIPAA.

True or False?

15. Written authorization is required for which of the following?

- a. Disclosures to another provider involved in the care of your patient
- b. Disclosures of psychotherapy notes
- c. Disclosures to indirect treatment providers
- d. All of the above

16. Therapists can share their passwords with the therapist assistants that are working with them so that they can both access the same files.

True or False?

17. Use or disclosure of a patient's demographic information for marketing purposes is allowed, but written authorization is required.

True or False?

18. Which statement is false, regarding the Notice of Privacy Practices?

- a. You must make a good faith effort to obtain written acknowledgement from patients
- b. Anyone can request a copy of your notice
- c. Your organization cannot treat patients who do not sign an acknowledgement

19. All covered entities must begin testing for the electronic transactions and code sets standards by April 16, 2003.

True or False?

Answers to the final exam

- | | |
|----------|-----------|
| 1. False | 11. False |
| 2. c | 12. d |
| 3. False | 13. True |
| 4. a | 14. False |
| 5. False | 15. b |
| 6. c | 16. False |
| 7. False | 17. True |
| 8. False | 18. c |
| 9. d | 19. True |
| 10. b | |



SAW



Related Products from HCPro

Books

The Long-Term Care HIPAA Lifeline: A Practical Guide on How to Comply

This book gives you HIPAA information the easy way—boiled down to the basics and written in plain English, making compliance as simple as possible. It is one of the few HIPAA products available on the market that is geared specifically for long-term care facilities. A bonus CD-ROM has all of the forms and checklists you'll find in the book, making it easier to adapt them to your facility's needs.

HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff

This convenient, pocket-sized handbook will help train department heads, nurses, LVNs/LPNs, therapists, and nursing managers on what it takes to comply with the HIPAA privacy regulations. It offers clear explanations and case scenarios on protecting resident confidentiality, recordkeeping, methods for protecting electronic information, and more. Trainers can even test staff on their HIPAA knowledge with a quiz found inside the handbook (answer key is included).

Newsletters

Briefings on Outpatient Rehab Reimbursement and Regulations

This monthly newsletter reports exclusively on federal regulations and reimbursement issues that affect rehab providers—and offers suggestions on how best to cope with these changes. Whether readers manage a rehab agency, outpatient rehab clinic, subacute care facility, or are in charge of their hospital's outpatient rehab services,

HIPAA Training Handbook for Rehab Providers

Briefings on Outpatient Rehab Reimbursement & Regulations keeps them on top of the ever-changing reimbursement policies and government regulations.

PPS Alert for Inpatient Rehab

This newsletter was created exclusively for inpatient rehab managers, therapists, nurses, or administrators who are involved with the completion of the new IRF-PAI form or who want to make sure they get the reimbursement their hospitals deserve. An eight-page, monthly publication, *PPS Alert for Inpatient Rehab* will become your survival guide when it comes to complying with inpatient rehab PPS.

Briefings on HIPAA

This newsletter was created exclusively for health care professionals who are in charge of information security or sit on information security task forces. It will help you comply with HIPAA, including establishing privacy-conscious business practices, restricting the amount of information that's used/disclosed to the minimum necessary, and more.

HIPAA Online Learning Courses from www.hcprofessor.com

Quickly and conveniently teach HIPAA compliance to all levels of clinical staff and employees . . . right from their own computers! Offer them these easy-to-understand, job-specific, customizable online training courses. Affordably train without the hassle of expensive consultants. No oversight is needed with these training modules. A final exam and student course history may be used to document training. The courses are always updated to reflect any changes to the HIPAA regulations.

Long-Term Care HIPAA Package

The Long-Term Care HIPAA Trainer's Toolkit

This kit makes training staff on the HIPAA privacy and security regulations easy. In this comprehensive, yet easy-to-understand group of resources, you'll get:

HIPAA Training Handbook for Rehab Providers

- **The Long-Term Care HIPAA Trainer's Playbook**
- 20 copies of **HIPAA Training Handbook for Long-Term Care: Privacy for Frontline Staff**
- 20 copies of **HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff: An Introduction to Confidentiality and Privacy under HIPAA**
- 10 copies of **HIPAA Daily Do's and Don'ts**, a 5" x 7" laminated cheat sheet to remind staff what they're allowed to do under HIPAA

Videos

HIPAA Privacy: A Compliance Overview

This educational video provides a thorough overview of the HIPAA privacy regulations and focuses on key points such as authorization, notice of privacy practices, penalties for noncompliance, information that can be released regardless of the patient's wishes, and patient rights. In addition, the video discusses what to do in case there is a violation, the role of privacy officials, and handling patient complaints.

ADLs and You: Breaking the Code

Not only will this video demonstrate how the ADLs are performed, it will also teach nursing home staff the importance of communicating ADL changes to nursing staff. It also encourages staff members to communicate on a regular basis to ensure accurate information is being coded.

Audioconference on tape

Secrets to Successful Therapy Billing for SNFs: Get Your Reimbursement

Are you positive that you are correctly billing for therapy services so that your skilled nursing facility (SNF) receives appropriate reimbursement? This 90-minute audioconference on tape features nationally respected experts who provide practical, how-to information and examples of best practices to help you make sure that you're billing correctly and supporting your billing with proper documentation.

CERTIFICATE OF COMPLETION

This is to certify that

_____ has read and successfully passed the final exam of
HIPAA Training Handbook for Rehab Providers

Suzanne Perney

Suzanne Perney
Vice President/Publisher