HIPAA compliance for outpatient rehab: Changing how we work in the privacy era

For all that technology has done to change the way we work and communicate, confidentiality remains a tenet of health care. But what was once a federally unregulated responsibility to protect patient privacy . . . is now a legal one.
Dear readers,

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has caused therapists and their office staff to become more vigilant in guarding their patients’ privacy. The act, which was passed in order to streamline the performance of health care transactions, has undergone more than a few changes since 1996. In the next 18 pages we show you how to comply. A special thank you goes to Gayle J. Holland, BSN, RN, CRN, director of corporate compliance and accreditation for the Polaris Group in Hingham, MA, who did a tremendous amount of work proofing the articles and making sure the information contained in them are correct.

Sincerely,

Byron Magrane
Associate Editor

Table of contents

Section I: Changing how we work
Practicing medicine in a new culture ........ 3
Timeline: Privacy or bust ..................... 4
Notice of privacy practices .................... 4

Section II: Privacy and liability
Privacy rules: Whisper while you work ........ 5
Protect patient privacy: Close the information gap 6
Penalty box .................................. 6
Exceptions to the privacy regulations ............ 7
Privacy principles ............................. 7

Section III: Patient consent
Hold the sides ................................ 8
Use and disclosure checklist ..................... 8
Remove identifying information ............... 8
Rev those risk assessment engines ............. 9
Dissecting disclosure ........................ 9
No labels .................................... 9
What to include in consent, authorization forms .10

Section IV: Business associates
A handshake won’t do ........................ 11
Become a watchdog: How to terminate agreements .................. 12
Business associates that do not require contracts ........... 12
Business associate research .................... 12

Section V: Overview of proposed security regulations
Guard those computer monitors ............... 13
Tips for electronically communicated information .................. 13
Termination protection ........................ 14

Section VI: Resources
Guidelines: Employee discipline for privacy breaches .................. 15
Security weaknesses ........................ 15
Hitting that HIPAA curve ..................... 16
How to become compliant ..................... 17
Disclosure mindset ........................ 17
Electronic signatures ........................ 17
Top 10 privacy essentials ..................... 18
Glossary .................................... 18
By the numbers ............................. 20
Changing how we work in the privacy era

Therapy’s latest regulatory responsibility, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), is spurring confusion within therapy practices. Many are in planning mode, others are angling to find a microwaveable template—some sort of “fill in the blank” policy they can zap into their practice culture with minimal effect on their resources.

Don’t do that.

“Office managers don’t even have the time for this,” says Dan Kelsey, a HIPAA trainer for the Indiana State Medical Association.

If time is what you’re worried about, consider this:

Even lawyers, who stand to make a bundle in counseling fees from the new law, are urging therapy practices to take a step back and simplify.

The truth is that therapy practices won’t have to pour hundreds of thousands of dollars into their practice to comply. Practices will not have to erect new walls to quiet the volume on their patient discussion. And no, they won’t have to turn their reception window into a peephole. The law is a bit of a paradox in that way.

Indeed, practices must obey the privacy and security laws and protect themselves through contracts should their business associates fail to comply with the law. But HIPAA is not asking you to crack a million piggy-banks, says Jen Urban, a lawyer with Foley & Lardner in Milwaukee.

There are small, cultural changes you’ll have to make—and revisions to vendor contracts—but that’s the crux of it.

Tweak policies, change the culture

Here’s the fact you don’t hear enough—most practices already have confidentiality protection measures in place. And most states have privacy-like laws for the health care industry. The only difference now is you’ll be federally regulated to protect patient information.

Therapists are legitimately worried about entangling their staff—and their reputations—in lengthy litigation if they fail to comply. But HIPAA doesn’t have to be the heavy burden therapists are making it out to be.

Some practices already have policies in place, and for those that don’t, unwritten codes typically guide how people protect patient information, reports attorney Abby Pendleton of Wachler & Associates in Royal Oak, MI.

Your mission now becomes one of research and preparation. To accomplish it, you must create a culture of caution—of thinking employees—who work together when handling a patient’s information.
Timeline: Privacy or bust

Editor's note: The Department of Health and Human Services approved the final draft of the Health Insurance Portability and Accountability Act of 1996’s (HIPAA) privacy rule in April 2001. The decision immediately put the onus on physician practices to develop policies and procedures, train employees, and amend business associate contracts by April 13, 2003—the compliance deadline. As of press time, this deadline remained intact, though minor amendments to the privacy rule were possible.

Patients are increasingly worried about who has access to their medical information. Take, for example, Alexandra Kantor of Reno, NV.

Kantor has recovered from a past illness. But several people found out about her condition. She doesn’t want to experience that feeling again. She, like many, worries that her personal health history could be used to deny her employment or insurance.

HIPAA’s privacy rule, finalized in April 2001, is designed to safeguard the records that hold this information—paper records, electronic records and oral communication.

Oral communication runs the gamut from paging patients, whispering in corridors, or using cell phones.

Confidential information is not necessarily relegated to a patient’s name. In fact, it includes information related to a person’s past, present, or future physical or mental health condition, and anything associated with health care services or treatment.

Patient-identifiable health information: What is it? Identifiable information is anything that can be associated with us—a name, address, and Social Security and phone numbers, for example.

There are several other identifiers that represent who we are, for example, a patient’s condition or the date of surgery. Releasing this information is a violation of the HIPAA privacy regulation.

Notice of privacy practices

The authors of the privacy rule want educated patients who can trust their providers and the organizations in which they work. To build trust, the privacy rule calls on covered entities to learn the rules and then live by them.

Organizations affected by HIPAA are required to issue a written notice to patients outlining their privacy practices.

The notice must

- inform patients of their rights
- disclose the organization’s privacy practices
- inform patients about the organization’s responsibilities under the law
- inform patients about all of the uses and disclosures of protected health information required or allowed by law
- explain the process for patients to access their medical records and amend their information

Patients can request the notice at any time, but you must provide it to first-time patients at the time they sign a consent form.

The rule also requires covered entities to “consider alternative means of communicating with certain populations.” This could mean Braille or notices posted in foreign languages.

All notices must be visible in high-traffic areas and posted on organization Web sites.

What’s more, the notice must explain how information will be used for fundraising activities. Sending fundraising materials to patients is allowed under certain restrictions. For example, patients must be given the option to decline receipt of any future fundraising-related mail, according to the law.
Privacy rules: Whisper while you work

Culture will define how well HIPAA compliance really works. For example, verbal exchanges of information—a critical form of communication in therapy practices—are covered under the privacy rule.

Practices must take measures to watch what they say, where, and with whom around the corner. Sound like a bad Abbott and Costello skit? It doesn’t have to be, says Annette Barreau, a health care attorney in Ft. Lauderdale, FL.

Therapy practices have always had to be careful with sharing patient information, particularly in verbal form. The invention of the glass partition in the waiting room served notice of this. But there are other risks.

Changing how we work
The privacy regulations are broad in many areas, including oral communication. But the current rule (amendments are possible) could restrict your assistant, for example, from saying a patient’s name out loud in the waiting area.

“That’s an extreme example, but possible,” explains Amanda Smith, a Charleston, SC, consultant.

Take the patient’s view. What can they hear? What can they see?

Several practices are already analyzing their privacy risks, a vital first step in the HIPAA compliance process. How are they doing this? They are becoming their customers: patients, vendors, cleaning people, pharmaceutical reps, even family.

During the working day, become the patient and do everything they do. That’s Sera Olivia’s HIPAA preparation at her physician practice in a Denver suburb. Although Olivia is a physician, you can still use her tips for your practice.

Applying the rules
Olivia offers the following tips to “becoming the patient” at your facility:

- Sit in the waiting room
- Go up to the reception window and ask a question
- Go back and ask a second receptionist a question when the first receptionist isn’t there
- Peer over the ledge to sneak a peek at paperwork
- Note whether there are any charts on the wall and whether you can see any names
- Take a chart and see whether your colleague notices

Once your therapist calls you in, drop your keys on the floor in front of a door. Is the door open? If so, can you see what, or who is inside? If closed, can you hear conversation?

Briefings on HIPAA

This 12 page newsletter was created exclusively for health care professionals who are in charge of information security or who sit on information security task forces.

It contains practical information, such as how to monitor audit trails of patient records, manage security incidents, and conduct educational awareness programs.

To order, go to http://secure.vscape.net/acb/showdetl.cfm?&Product_ID=54&DID=90, or call our Customer Service Department at 800/ 650-6787.
Protect patient privacy: Close the information gap

Before you determine the security and privacy measures needed to protect patient information, you have to assess what you already have. Lawyers call this assessment a gap analysis.

Practice-wide compliance effort
Review your confidentiality policies to find out where you are. Review all your policies—even those outside the general compliance function, says Richard Kusserow, former U.S. Inspector General, who is now president of Strategic Management Systems, Inc.

A Health Insurance Portability and Accountability Act (HIPAA) compliance program has to mesh with the rest of the compliance effort within the practice, says Kusserow. If you view HIPAA as another policy requirement, you’re walking down a dangerous path. Too much decentralization could produce a cadre of conflicting policies saying similar things and giving mixed messages, Kusserow warns.

Another mistake: developing a single privacy policy and having your staff sign an agreement that holds them accountable for the privacy of health information. This is not enough.

At a recent compliance summit in Washington, DC, Kusserow pointed out that many providers only go through the motions. It’s one thing if you get every employee into a room to talk about what privacy means. It’s something else if the program is ineffective.

“If you’re not going to be serious, then don’t do it, because you’re going to get yourself into more trouble if you go halfway,” says Dan Kelsey, a trainer with the Indiana State Medical Association.

Kusserow agrees: An ineffective program that does not protect your patients’ information is as good as no program at all.

Hotlines, internal pop-quizzes masked as surveys, questionnaires to outside vendors, and periodic seminars are among the ways to measure the effectiveness of your HIPAA compliance program.

Identify risk areas
Define your risk areas before you set policies—and do it before you educate the staff and scare them with stories of potential litigation. “You need buy-in,” Kusserow says. “And to get it you first have to find out where you are and where you need to go.”

The practice has to do its homework, assess its risk areas, and identify its business and vendor relationships. Since each practice is responsible for the actions of its business associates, lawyers play a key role here. They can pore over information to make sure your practice is fully protected and change broad, loosely interpreted contract language that could get you in trouble.

Take Michael Marshall, privacy officer at Kennedy Orthopedics, a mid-sized practice in Trenton, NJ, for example. He’s met with his physician administrative staff to review every possible risk area in his 26-provider office. What he talks about applies to therapists as well. Supplying crayons and oak tag paper; Marshall

---

Penalty box

HIPAA outlines the following wrongful disclosure penalties for physicians who knowingly disclose patient information:

- **Misuse of health information**
  Penalty: Fines up to $50,000/imprisonment for a term of up to one year

- **Misuse under false pretenses**
  Penalty: Fines up to $100,000/imprisonment for a term of up to five years

- **Misuse with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm**
  Penalty: Fines up to $250,000/imprisonment for a term of up to 10 years

---
Changing how we work in the privacy era

asked the staff to draw pictures mapping out how information flows within the practice. He assigned people to cover different communication areas: paper flow, electronic flow, verbal communication. It was a fun project that served as a great starting point. Marshall repeated the drill to map out external relations with business associates and vendors.

Redefining job duties
Marshall’s plan started well before the coloring exercise. In the spring, he took a composite of all job descriptions. He asked employees to write out their primary and secondary duties and to identify the information they see every day, where they see it, and why they need it. Then the million-dollar question: “Do they need it?”

“You may think every single employee in your practice is honest and won’t touch the medical information,” says Toni Alexander, a compliance officer for Cardiac Rehabilitation Center in Dover, DE.

“But what about unintentional misuse like leaving a folder in the wrong place for the cleaning guy to snatch . . . or the sheer possibility someone could get to information they don’t need to know about?”

---

### Exceptions to the privacy regulations

Health information can be used without patient authorization under the following circumstances:

- Public health activities, such as reporting diseases or collecting vital statistics, required under state and federal law
- Health oversight, including civil and criminal proceedings, inspections, and audits
- Law enforcement: Disclosures may be made to law enforcement officials pursuant to a warrant, subpoena, or order issued by a judicial officer
- To coroners, medical examiners, funeral directors, and government authorities
- Organ and tissue procurement organizations

---

### Privacy principles

When the Health Insurance Portability and Accountability Act of 1996 was first passed, the law required the Department of Health and Human Services to develop privacy principles for Congress to use in drafting legislation. Delivered to Congress in 1997, the principles established a context for a more thorough understanding of the privacy rule. Here is a summary of the 58 standards in the privacy rule:

**Boundaries.** Individual health care information should be used for health purposes only, subject to a few carefully defined exceptions.

**Security.** Federal law should require those to whom we entrust health information to protect it against deliberate or inadvertent misuse or disclosure.

**Consumer Control.** Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them.

**Accountability.** Those who misuse information should be punished, and those who are harmed by its misuse should have legal recourse.

**Public Responsibility.** Privacy must be balanced by public responsibility to contribute to the common good. This includes oversight, public health, research, and law enforcement.

This list comes from HIPAA Made Simple, A Guide to Compliance by Margret Amatayakul, MBA, RHIA, FHIMSS. Visit www.hcmarketplace.com or call 800/650-6787 to order your copy today.
HIPAA compliance for outpatient rehab

Hold the sides
Minimum necessary rule manages what can and can’t be disclosed

The staff at your facility must make a reasonable effort to disclose or use only the minimum amount of protected health information necessary to do their jobs. According to the law, they can disclose information requested by other health care providers if the information is vital for treatment. To determine what is necessary to be disclosed and what should be withheld, consultant Amanda Smith offers the following question test:

- How much information are you planning to use or disclose?
- By using the information, will the number of people who are likely to have access to that information increase?
- How important is it that I use/disclose this information?
- What’s the likelihood that further uses or disclosures could occur?
- Where is the information being disclosed (location), and in what form (e-mail, conversation)?

Use and disclosure checklist

Allowable uses
The following is a list of allowable uses of protected health information (PHI) not requiring patient authorization:

✔ Judicial and administrative proceedings
✔ Law enforcement
✔ Emergency circumstances
✔ To provide information to next-of-kin
✔ Identifying a deceased person, or the cause of death
✔ Treatment
✔ Payment
✔ Health care operations
✔ Oversight of health care system
✔ Public health functions

Disallowable uses
These require individual authorization before the information can be used or disclosed.

✔ Use of PHI for marketing of health and non-health items and services
✔ Disclosure of PHI for sale, rent, or barter
✔ Disclosure of information to an employer for use in employment determinations
✔ Use or disclosure of information for fundraising

Source: North Shore Medical Center, Inc., physician practice education program. Reprinted with permission.

Remove identifying information

Each patient’s case dictates what remains in the medical record. For example, if you are performing a study based on a rare diagnosis, after withholding the basic information, you would be left with patient-related diagnosis information, such as symptoms, procedures, physician’s notes, and history—but nothing to identify the individual patient subject.

A full list of identifiers includes the following:

- Name
- Address (including street address, city, county, ZIP code)
- Names of relatives and employers
- Birth date
- Telephone numbers
- Fax number
- E-mail address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web URL
- Finger or voice prints
- Photographic images
Therapy practices may use protected health information (PHI) without patient authorization if the information is de-identified—that is, if the information does not identify any patients. PHI may include fragments of data apart from one’s name that, when pieced together, can sometimes identify a person. Here is an example of data that seems innocent, but could identify a patient:

A therapy practice performs a certain type of procedure one day a week—and only one on that day. Someone may be able to piece together, from admission records, the name of the individual who underwent the procedure. The person’s medical records could be identified even if the individual’s name, address, and Social Security number aren’t in the medical information.

According to Foley & Lardner attorney Jen Urban, de-identified information has to be completely stripped down so that no one is able to piece things together and identify someone.
Consent and authorization do not overlap under the privacy regulations.

Providers must receive consent from patients “prior to using or disclosing protected health information to carry out treatment, payment, or health care operations,” according to the privacy rule.

Authorization, meanwhile, is required for the use and disclosure of health information for all other purposes, such as employment determinations and marketing and fundraising activities not specified in the regulations as part of health care operations.

Guidelines for consent forms
The proposed regulations allow organizations to use a single form to achieve consent for several things.

However, if a provider chooses to also use the form for consent with activities beyond routine treatment, payment, and health care operations, it must organize the form in such a way that it is clear to the patient that he or she is consenting to several different disclosures.

For example, if the form is used to obtain required consent to share a patient's HIV/AIDS information, this consent must be “visually and organizationally” separate from other consents or authorizations and must be separately signed and dated by the individual. The proposed rule also requires that consent and authorization forms be written in “plain language.”

The Department of Health and Human Services (HHS) has not offered model forms to use as templates for providers.

However, a spokesperson for the agency indicated that HHS will provide “guidance” on drafting consents, likely to come prior to the date the regulation becomes enforceable.

Providers can require patients to sign a consent form to receive treatment. That’s not the case with authorizations, according to Chris Zakrzewski, senior counsel with Foley & Lardner in Denver.

Anatomy of an authorization form
The proposed HIPAA privacy rule prescribes a minimum set of elements to be included in all authorizations:

1. A specific description of the information to be used or disclosed. There are no limitations on the information that can be authorized for disclosure. An individual can authorize a covered entity to disclose his or her entire medical record if that is specified in the authorization.

2. The name or specific identification of the person(s) or class of persons that are authorized to use or disclose the protected health information.

3. The name or specific identification of the person(s) or class of persons to whom the physician practice is authorized to make the use or disclosure.

4. An expiration date or event. This can be a specific date, a specific time period, or an event directly relevant to the individual or the purpose of the use or disclosure.

5. Statement saying that the individual has the right to revoke an authorization in writing. However, once the information has been used, the patient cannot revoke authorization.

6. An explanation that when the information is used or disclosed following the authorization, it may be subject to redisclosure by the recipient and may no longer be protected by this rule. “Once the information is disclosed to a third party, they may in turn disclose it to someone else and they may not be a covered entity under HIPAA,” said Zakrzewski. “The patient has to know that.”

7. The individual’s signature and the date of the signature. If the authorization is signed by a personal representative of the individual, the representative must indicate his or her authority to act for the him or her.
A handshake won’t do
Revise contracts with business associates

Old Saint Nick makes a list and checks it twice. You should do the same when determining who your business associates are, and what they do with patient information. This is the advice from attorney Amy Fehn of Wachler & Associates in Royal Oak, MI.

The Health Insurance Portability and Accountability Act of 1996 is designed to protect communication with business associates such as lawyers, actuarial professionals, accountants, health care consultants, and billing companies.

In other words, if you have a contract with someone helping you to do your job, he or she qualifies, according to Pendleton. The list is potentially endless. “It may just take a little tweaking in the contract at the time of renewal to make sure the language is specific and the law is being followed,” she says.

Therapy practices need reasonable assurances that the information they are sending out is getting the same confidentiality overcoat as it is in their own office. Take software vendors. Each performs certain functions that need patient information.

“I bet there are individuals who have access to [protected health information (PHI)] but don’t need access . . . that has to change,” Pendleton says.

Therapists cannot disclose PHI to business associates unless the two parties have a contract.

Each contract must contain a confidentiality clause that holds these associates accountable for PHI.

The associate cannot use or further disclose the information in a manner that violates the privacy rule. To be on the safe side, limit information provided to business associates to de-identified material.

At the termination of contracts, business associates must return or destroy all PHI within a reasonable amount of time. They cannot retain a single copy. -

Who’s on your list?
✓ Auditors
✓ Billing firms
✓ Clearinghouses
✓ Consultants
✓ Lawyers
✓ Separate collection agencies
✓ Shredding companies
✓ Software vendors
✓ Therapy contractors and vendors

Need more copies? That’s easy

If you’d like to order extra copies of this special report, please use the coupon below or call our Customer Service Department at 800/650-6787. Extra copies are $39 each.

❑ I’d like ________ copies. The price is $39 each.
❑ Payment enclosed.
❑ Please bill me. Please bill me using PO #
 Charge _______ AmEx _______ MasterCard _______ VISA _______
 Signature ____________________________________________ (Required for authorization)
 Card # ___________ Expires ______________
 (Your credit card bill will reflect a charge to “Opus Communications.”)

Name & Title ___________________________________________
Organization ___________________________________________
Address _______________________________________________
City __________________________ State _______ ZIP ___________
Phone ( ) ___________ Fax ( ) ___________
E-mail ________________________________________________________

Mail to: Call: Fax: Internet: E-mail:
Opus Communications, a division of HCPro 800/650-6787 800/639-8511 customerservice@hcpro.com www.hcmarketplace.com
P.O. Box 1168, Marblehead, MA 01945
R0001

Changing how we work in the privacy era 11
You are your partner’s keeper. The Department of Health and Human Services (HHS) plans to issue fines for a negligent violation of a single Health Insurance Portability and Accountability Act of 1996 privacy standard. If nothing else, this should be the impetus to get your business partner agreements up to speed. Under the proposed rule, providers can’t be held responsible for their business partners’ confidentiality breaches, provided they follow certain steps and develop contracts with specific privacy provisions.

Marilyn Lamar, partner in the Chicago office of the law firm McDermott, Will and Emery, recommends using a contract addendum. Since many business associate contracts are drafted with “evergreen” provisions that roll over automatically unless they are cancelled, attach a contract addendum to protect your practice.

Terminate agreements
If a business associate violates the privacy rule, the organization under contract with the business associate can be held responsible for the non-compliance—unless the organization takes the appropriate steps.

According to Lamar, if your organization becomes aware of a breach by a business associate, it must take one of two steps to fix the breach:

- Terminate the agreement
- Report the breach to the HHS (if termination is not feasible)

If your business associate is the sole provider of a service or if other extenuating circumstances make immediate termination difficult, the final rule allows for continuation of the business relationship as long as the breach is reported.

Business associates that do not require contracts

- Employees.
- Contracted employees who perform a substantial portion of their work at the physician practice (i.e., physical therapist). Remember that without a contract, the Department of Health and Human Services will consider these professionals as members of the work force.
- Oversight agencies.
- A hospital, unless the hospital performs billing services for staff providers.

Business associate research

Before meeting with an attorney to rework business associate contracts, consider asking your associates the following questions:

- What do you see as your obligations under the privacy and security regulations?
- How do you plan to limit the use and disclosure of protected health information (PHI) by your subcontractors and agents?
- Did you change operational practices in preparation for the Health Insurance Portability and Accountability Act of 1996?
- What security measures do you have in place to safeguard PHI?
- Do you have an education program specifically for these regulations? Who’s giving it, when, and what is the substance of the training?

Guard those computer monitors

Creating secure computer stations and minimizing the threat of unauthorized access are critical under the Health Insurance Portability and Accountability Act of 1996’s (HIPAA) proposed security regulations, which may be finalized this year as part of a sweeping effort nationally to protect health care information.

Workstation positioning is crucial, according to privacy officer Christa Steene of the Prevea Clinic in Green Bay, WI. Computer screens should not be easily visible (or readable) to the public or coworkers.

Tips for electronically communicated information

E-mails may seem like a safe way to communicate, but electronic transmission is only as safe as the person on the other end.

Physicians must make sure their colleagues follow the privacy rules or the system doesn’t work, according to attorneys with Davis Wright Tremaine, who spoke during a compliance conference in Washington, DC, last year.

Avoid the following practices:

- Leaving a patient’s medical file on the computer screen while you go down to the cafeteria
- Leaving your computer logged in to the medical records database
- Leaving hand-held dictation devices unattended
- Using passwords that include your last name

One option offered by Kate Borten of The Marblehead Group, a Massachusetts consulting firm: Put polarized filters on your computer screens. These filters make computer screens readable only when looking at the screen straight on.

Also consider exposure from windows. People walking near your building may be able to read what’s on computer screens that face the windows, explains Borten. If they can, you’ll need to rearrange your setup.

Log on, log off

Although the proposed security rule requires employees to log off of terminals when they leave them unattended, there are more practical security measures for those two-minute coffee breaks.

Two considerations: a password-protected screen saver or keyboard-lock feature. Workstation lockdown devices are especially important for personal digital assistants (such as Palm Pilots), Borten says.

Numerous lockdown devices are available—from a cable lock with a combination or key lock to alarms.

“These are the kinds of things that you’d want to have in an information security program today—HIPAA or no HIPAA.”
Termination protection
What should be included in termination policies and procedures?

When you fire or lay off employees, you need to do more than take their keys and escort them to the door. Thorough termination policies and procedures are essential to protect the privacy of patient health information.

And these policies and procedures are now required under federal law—the Health Insurance Portability and Accountability Act of 1996 (HIPAA). According to the proposed security rule, termination “procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access it.”

HIPAA’s mandatory termination requirements include the following:

- Changing combination locks
- Removing the employee from access lists
- Deleting the employee’s user account(s)
- Collecting keys, tokens, or cards that allow access

Without termination policies and procedures that are strictly followed, you leave yourself vulnerable, says Holly Ballam, corporate privacy officer for Beth Israel Deaconess Medical Center in Boston. Terminated employees, “could walk back into the office two, three years later, and [their] passwords could still work and they could get information on their neighbor, a relative, anybody.”

A closer look at the benefits
It’s hard to say how big the risk is that terminated employees will retaliate by causing harm to their former employer, adds John Christiansen, partner at Stoel Rives LLP, in Seattle.

All the same, termination policies and procedures are beneficial because having the process in writing helps therapy facilities apply practices more consistently, he says. And in being consistent, practices have more power to fight discrimination claims. Develop a step-by-step process that clearly indicates which people are responsible for which activities. Inadequate communication between human resources and the receptionist could cause a problem.

Keys and combinations
Don’t give employees any warning that they are about to be fired, says Christiansen. This is particularly important for employees in sensitive positions with access to medical records.

Track what access tools employees receive so that if termination is necessary, you can collect everything they have received.

User accounts and access lists
Removing the employee from user accounts and access lists, “is always a sensitive situation,” says Christiansen.

Make sure all access privileges on the network are terminated with minimal warning, but “you don’t want to suddenly freeze the person out of their computer without them knowing what’s going on,” he says.

Develop a checklist as your practice goes through the termination procedures, Ballam says. The checklist will help you to be certain that everything is done before the employee leaves the building.

Resources for this report
complianceinfo.com
himinfo.com
hcmarketplace.com
Briefings on Outpatient Rehab
Reimbursement & Regulations
Guidelines: Employee discipline for privacy breaches

As your organization develops its policies and procedures for applying sanctions, consider how others tackled the task. Keith MacDonald, a senior manager with First Consulting Group in Lexington, MA, worked with a team of colleagues to develop these sample guidelines for Harvard Vanguard Medical Associates in Boston:

Level I

Inadvertent breach of privacy: accidental, often due to lack of education or awareness. Examples of this may include failing to log off a computer terminal or sharing passwords. Often these breaches do not result in actual patient information being exposed or shared. Punishment might include a verbal warning and mandatory reeducation for first offense up to termination for repeated offenses.

Level II

Intentional breach without malice: accessing a patient record with no legitimate business purpose for doing so. This might mean accessing a friend’s or relative’s record out of curiosity or releasing patient information inappropriately. Punishment might include written warning for first offense up to termination for repeated offenses.

Level III

Intentional breach with malice: accessing a patient record with the intent to use it for personal gain or to harm someone. Punishment would include termination for cause.

Security weaknesses

Portions of the following list of real life security breaches were presented to physician practices in June 2001 by Brian Kozik, compliance officer with the North Shore Medical Center in Salem, MA. Although most of these maladies happened to patients of physicians, similar foibles can happen to your patients as well, if you aren’t careful.

Improper disposal

• A physician practice accidentally left patient records on an old computer that was sold at an auction.
• A diskette containing medical records was found on the curb outside a physician’s office. The diskette slipped into the recycling bin and then fell out.

Improper disclosure

• Misrouted faxed medical records ended up in the hands of a pharmaceutical company sales staff.
• Employee sent HIV records to a Florida newspaper that said it was doing a story on the virus and needed statistics. The paper promised names wouldn’t be used. But the reporters called the people on the list.

Improper access

• Medical student copied health records and sold them to malpractice attorneys.
• Physician tossed an outdated patient file in the trash can in the men’s room. The cleaning people found the file and recognized the name.
Hitting that HIPAA curve
It’s not official yet: Beware of what is coming in the months ahead

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules for privacy are like a living, breathing organism, as new modifications are added and taken away to make the legislation more patient- and facility-friendly. The following are a list of modifications to the current privacy regulation being considered by government agencies:

- **Consent notice.** After looking at the original version of the privacy regulations, there are some legislators who feel current consent requirements limit access to care. In order to improve the access to care, they want to remove these requirements. Under the new proposal, patients would be asked to acknowledge the receipt of the privacy rights and practice. “What they are saying is, instead of having consent for everything that would affect care delivery, the requirements would be for providers to notify their patients when admitted,” says Gayle J. Holland, BSN, RN, CRN, director of corporate compliance and accreditation for the Polaris Group in Hingham, MA.

However, it only applies to the use of disclosures for treatment, payment, and health care operations, such as treatment payment and care delivery. Authorization will still be needed for non-health care operations, such as asking the patient to be a part of marketing copy.

- **Change to minimum communication.** The proposal retains the oral communication and minimum necessary requirements of the original rules—no discussion of patients’ conditions is allowed. The biggest change is that a therapist can discuss his or her patients’ treatment with other therapists and professionals without violating the rule.

- **Business associates.** The rule currently requires covered entities to have contracts with all business associates to ensure patient privacy. The proposed rule calls for a model business associate contract and gives organizations a year to change their existing contracts. The Department of Health and Human Services (HHS) “would give you something to use as an addendum that would give you the language as well as another year, before you could be fined,” Holland says.

- **Marketing.** Instead of obtaining the specific authorization before sending marketing materials, the proposed rule allows for therapists to communicate freely about treatment options and other health-related information.

- **Uses and disclosures for research purposes.** This proposal would eliminate the need for researchers to use multiple consent forms for research purposes. In lieu of this, they can use a single combined form. It will also simplify other provisions so that the existing rule more closely follows the common rule that governs research.

- **Alternative approach to deidentification.** HHS is seeking comments on establishing a limited data set that does not include directly identifiable information. “What you are going to have to do is make [documents] not reidentifiable,” says Holland. “For instance, if you want to study something about people who are under Part B, you are going to have to get their Medicare number. And the reason you can do this is for aggregate data or to set benchmarking. It all boils down to this: You can still get information, you just have to promise not to reidentify it and contact that person.”

- **Uses and disclosures of patient data for which authorization is required.** Authorization is only needed in one permission form for a specific use or disclosure of patient data. In the original privacy rule, this was not permitted. Patients will still have to grant advance permission to therapists for each use or disclosure. This will eliminate the need for organizations to use different types of forms to get said permission.

- **Accounting for disclosures of protected health information.** The proposal would not require organizations to account for disclosures in which the
individual provided written authorization. The current rule states that even if you have patient authorization and you want to disclose something, you have to report it to the patient. The proposal clarifies that covered entities can disclose protected health information for the treatment and payment of certain health care activities of another health care provider.

The comment period on these modifications ended in April and HHS Secretary Tommy Thompson says at least four months will be needed to review the comments.

How to become compliant

The following are four tips that will get you moving toward the Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance:

1. Know the details of how your facility uses protected health information in its day-to-day operations, says Tracy Field, MS, JD, chair of the HIPAA task force for Arnall Golden Gregory, LLP, in Atlanta. “You have to take a step back and analyze what you do and how you would be regulated under HIPAA.”

2. Seek training once you have decided where your facility fits in under the HIPAA umbrella. Attorney George Olsen, of Williams and Jensen in Washington, DC, says a lot of critical information on rule compliance will be released within the next year.

3. Unless you submit a plan to the Department of Health and Human Services (HHS) explaining why you can’t meet the compliance deadline for the transaction and code set regulations, know that it occurs this October. Items such as your budget and a timeline showing when you will start testing interoperability between you and your payers are what HHS wants, Field says. Remember, if you don’t submit the plan and you don’t meet the October deadline, you will be in violation. A model plan is on the HHS Web site at www.access.gpo.gov/su_docs/fedreg/a020415c.html. To view the plan, click on “health insurance reform; electronic transaction standards; model compliance plan,” under the CMS headline to access the model compliance plan and extension form.

4. If all of your patient records are electronic, check the types of firewalls you have, what kind of access controls you have, and your operating procedures.

Disclosure mindset

When faced with a request to disclose health information, ask yourself these five questions:

- Who is making the request?
- Do they have the right to accept the information—for example, can you identify him or her?
- Will disclosure violate the patient’s right to privacy?
- Is there a risk that the disclosure will harm the patient in some way?
- Does the patient consent to the disclosure?

Electronic signatures

With more health care organizations using electronic signatures, the need for security has become crucial. An electronic signature verifies a practitioner’s identity, thus creating an individual “signature” on computer-based records. According to the Health Insurance Portability and Accountability Act of 1996’s security standard, electronic signatures, which range from biometric to digital signature devices, must do the following:

- Identify the signatory individual
- Ensure the integrity of a document’s content
- Provide evidence that will make it difficult for the signer to claim that the electronic representation is invalid
Top 10 privacy essentials

The following are the most important privacy essentials to remember as your therapy practice begins to implement the cumbersome legal requirements:

10. Do not send mass mailings to your patients without first checking the Health Insurance Portability and Accountability Act of 1996 “marketing” restrictions.

9. Maintain strict disciplinary policies for breaches of confidentiality. Enforce them.

8. Make sure new employees are adequately trained on privacy policies and that all employees receive updates/reminders.

7. Be aware of confidential information that is being placed in trash cans and recycle bins or boxes—utilize a shredding service if necessary. Make sure you have a contract with that shredding company.

6. Avoid placing patient information in view of other patients or family members (e.g., sign-in sheets in waiting rooms, computer monitors with patient information in plain view of other patients and family members).

5. Limit the amount of unnecessary information access given to employees.

4. Use caution when sending faxes containing patient information (be aware of who may be viewing the information from both ends).

3. Protect medical records after hours (e.g., be aware of cleaning and maintenance people inside the office after hours. Would it be easy for them to look at records or other confidential patient information?).

2. Emphasize the need to maintain confidentiality of passwords (e.g., no sharing of passwords, no posting of passwords on computer monitors).

1. Emphasize the importance of confidentiality in oral conversations (e.g., discourage gossip, and limit hallway, elevator, and parking lot discussions).

Source: Health care attorneys Amy Fehn and Abby Pendleton of Wachler & Associates in Royal Oak, MI. Reprinted with permission.

Glossary

Interpreting how the final privacy rule defines certain words will go a long way in helping you understand your obligations under the law. The following list of privacy rule definitions include some of the more important terms for therapy practices (additional information about the definitions appears in italics):

1. Individually identifiable health information
   “A subset of health information that identifies the individual.” This can include demographic information “collected from an individual, created or received by a health care provider, health plan, employer, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual; or that relates to the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

2. Protected health information (PHI)
   Individually identifiable health information that is
   • transmitted in electronic form, such as e-mail
   • maintained in any medium described in the definition of electronic media under the Health Insurance Portability and Accountability Act of 1996

   Education records covered by the Family Educational Right and Privacy Act are not included in PHI

3. Business associates
   “Those who perform or assist covered entities, such as physicians, in performing activities that require the use or disclosure of patient-identifiable health information. The information includes claims processing, data analysis, billing, practice management, or repricing.”

   Business associates do not include employees and volunteers of the physician practice.

4. Disclosure
   The release or transfer of information outside the practice. Disclosure also means giving someone access to the information, or divulging it in any other manner.
5. Health care
“Care, services, or supplies related to the health of an individual,” including but not limited to the following:

- “Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care
- Counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.”

6. Health care operations
- “Quality assessment and improvement activities, population-based activities, and related functions that do not include treatment
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs
- Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs
- Business planning and development
- Business management and general administrative activities of the entity including management activities, customer service, resolution of internal grievances, due diligence”

7. Health information
“Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.”

“This information must relate to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

8. Marketing
“Communication about a product or service, the purpose of which is to encourage recipients of the communication to purchase or use the product or service.”

9. Psychotherapy notes
“Recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.”

Besides content, the key to the definition of psychotherapy notes is the requirement that they are separate from other information and records, according to the American Health Information Management Association. If such notes are maintained in another or with another record, they are no longer covered by this definition.

10. Transaction
The transmission of information between two parties to carry out financial or administrative activities related to health care. This includes the following types of information exchanges:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments

11. Treatment
“The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.”

continued on p. 20
HIPAA compliance for outpatient rehab

400,000 Dollars that a small physician practice has projected to spend to comply with the security and privacy regulations. Accounting for the large sum: a new medical records storage and disaster prevention system.

0 Common sense a practice has if it is small or even mid-size spending that kind of money, says Michael Davis, compliance officer of Adventist Health Medical Group in Portland, OR.

“Leaving your privacy and security policies on the shelf won’t fly, says Brian Kozik, compliance officer for the North Shore Medical Center in Salem, MA. Incorporate policies into the culture—spend money for practical changes to help you meet the standards, says Kozik.

2 to 10,000 Dollars that practices may need to budget to comply with the security and privacy regulations, according to a survey of HIPAA attorneys.

*75 to 200,000 Dollars that a typical 50-physician practice could spend to upgrade and change internal billing systems, referral authorization procedures and claims status checks to comply with the law’s standardized electronic formats.