Safeguarding Visual PHI from Prying Eyes

In a previous issue, we discussed what a health care organization must do to minimize the risk that legitimate oral communications of a patient’s protected health information (PHI) will be overheard. Generally, overheard disclosures—known as “incidental disclosures”—won’t violate the HIPAA privacy regulations, as long as your organization makes “reasonable efforts” to limit their likelihood. (See “Safeguarding PHI that’s Communicated Orally,” Trainer, June 2004.)

Similarly, the HIPAA privacy regulations require a health care organization to minimize the risk that legitimate visual communications of a patient’s PHI will be seen by those not authorized to see it. This training session focuses on how to safeguard visual PHI from accidentally being seen by people who aren’t authorized to have access to it. Visual PHI generally includes PHI that’s visible in any form, whether it’s written on paper, printed on a prescription vial, or displayed on a white board or computer monitor. For example, in some physicians’ offices, patient charts are placed in chart holders located on or next to the doors of patient exam rooms. If patients’ charts are visible to anyone walking by the exam room, one patient may see another patient’s PHI.

To help you understand what you must do to safeguard PHI and minimize the risk that visual PHI will be seen by those not authorized to see it, we’ll give you 14 rules to follow. There’s also a Trainer’s Quiz to help you test your knowledge.

14 RULES FOR SAFEGUARDING PHI FROM PRYING EYES

To help you protect the privacy of visual PHI, follow these 14 rules.

**Rule #1: Limit PHI Written on Sign-In Sheets**

Many health care organizations ask patients to write their names and arrival times on a sign-in sheet. This is okay, as long as you limit the amount and type of PHI disclosed, said HHS’s Office for Civil Rights in the answer to one of its “frequently asked questions” (FAQ). For example, don’t ask patients to write down the reasons for their visits.

*Example:* Dr. X’s office asks all patients to sign in at arrival. The sign-in sheet has a place for the patient’s name and time of arrival, and can be viewed by each patient who signs it. This disclosure is permissible under the HIPAA privacy regulations. But it wouldn’t be appropriate to require patients to write down any
It’s also a good idea to keep sign-in sheets in a location that’s accessible only to patients who are signing in. Don’t place sign-in sheets where they may be in clear view of others.

An even better approach is to use a sign-in sheet with removable labels, says HIPAA security consultant Lesley Berkeyheiser. Once a patient has signed in, the label can be removed from the sign-in sheet and attached to a list kept behind the reception desk. That way, patients signing in can’t see the list of patients who’ve already signed in that day.

**Rule #2: Limit PHI Posted at Entrances to Patients’ Rooms**

The HIPAA privacy regulations don’t prohibit health care organizations (like hospitals and nursing homes) from posting patient names on or near the doors to patients’ rooms. In fact, posting names may be necessary for treatment purposes (say, to make sure that staff provide patient care to the correct patient) or for health care operations purposes (say, as a service for patients and their families), according to an answer to a FAQ posted by OCR. It may also be necessary, says the FAQ, to post patient care signs (like “high fall risk” or “diabetic diet”) at patients’ bedside or at the entrances to their rooms.

But you should limit the PHI you disclose this way to the minimum necessary for the purpose of the disclosure, according to the FAQ. For example, hospital employees may need to know that they must take special infection control precautions before entering a patient’s room, but they don’t need to know the nature of the patient’s infection.

**Rule #3: Get Patient’s Written Authorization Before Posting Cards, Letters, or Photos**

If a patient sends you documents containing PHI (such as cards, letters, notes of appreciation, or photographs), get the patient’s written authorization before posting them on an office bulletin board that’s visible to or accessible to patients and visitors, says Berkeyheiser. She notes that some organizations don’t think it necessary to get an authorization to post these items on an office bulletin board. But in these situations, PHI (such as the patient’s name, address, and physical characteristics) is being disclosed to others. So the HIPAA privacy regulations require you to get the patient’s authorization, Berkeyheiser believes. She points out that the regulations require health care organizations to get a patient’s written authorization to disclose her PHI (including photographs) for purposes other than treatment, payment, or health care operations.

**Example:** XYZ Dental Group has a bulletin board in its patient waiting room that displays patient photographs. Patient A sends the group a photograph with her new smile, along with a letter of appreciation. But the group doesn’t post it right away. When Patient A arrives for her next visit, the receptionist asks Patient A to sign a form that authorizes the group to post her let-...
ter and photograph on the bulletin board. If Patient A signs the form, XYZ Dental Group can post the letter and photograph on its bulletin board.

**Rule #4: Avoid Placing X-Ray Light Boards or White Boards in Common Areas, and Keep PHI to Minimum If You Do**

Don’t place X-ray light boards or white boards (also called dry erase boards) containing patients’ PHI in common areas when possible. Instead, place them in an area generally not accessible by or visible to the public, suggests another FAQ posted by OCR.

Health care providers may sometimes find it necessary, for patient care purposes, to locate white boards where visitors and other patients may see the information (for example, in an emergency department). If you need to do this, limit the PHI disclosed on the boards to the minimum necessary for the purpose of the disclosure. In other words, list only the information needed to locate the patient and coordinate work assignments (say, patient name, room number, and attending physician). One way to enhance patient privacy when using white boards is to list only a patient’s first name and last initial, rather than the patient’s full name, says HIPAA consultant Mary Brandt.

**Rule #5: Keep Patient Charts at Central Location if Possible**

If possible, keep patient charts at one central location that isn’t accessible to patients or visitors. For instance, a medical practice can keep the charts of all the current day’s scheduled patients together in a file box in the main reception or medical records area. This practice allows easy access for staff, but not for others. A provider can simply pull the chart she needs before seeing a patient.

In a hospital, keep all patient charts at the nurses’ station when possible, where providers may pick up a chart before visiting a patient. Just make sure there’s someone at the nurses’ station at all times who’s authorized to retrieve patient charts immediately for providers, says health information consultant Tom Hanks. Otherwise, the policy can impede a provider’s access to a patient chart and hamper or delay patient care, he warns. And, of course, make sure the charts at the nurses’ station aren’t readily visible to anyone who might walk by.

OCR’s answer to another FAQ gives the following examples of additional measures that may be reasonable and appropriate for a health care organization to take to safeguard patient charts:

- Limit access to certain areas;
- Supervise the areas where charts are located; and
- Escort visitors in the area (see Rule #14).

**Rule #6: If You Must Leave Patient Chart in Holder Outside Exam Room, Keep It Covered or Turned Around**

In some treatment situations, it may not be practical to keep charts at a central location. For example, many health care organizations place patient chart holders (also called wall pockets) in or near exam rooms to give physicians convenient access to the medical information they’ll need to examine or treat a patient. In a physician’s office, these chart holders are located on or next to the doors of patient exam rooms. Similarly, in a hospital or nursing home, chart holders are often placed right outside patients’ rooms or near their beds. Placing patient charts in chart holders is okay, as long as your organization takes reasonable and appropriate measures to safeguard the privacy of each patient’s chart, according to a FAQ posted by OCR.

What’s a reasonable and appropriate safeguard? The HIPAA privacy and security regulations don’t say. Instead, they leave it up to each organization to set policies and procedures that will work best for it. An answer to a FAQ says that it may be reasonable and appropriate for a health care organization to protect a patient chart from view by placing it in the chart holder with the front of the chart facing the wall—or by keeping the front of the chart covered. You can also use opaque chart holders to protect charts from view, says Berkeyheiser.

**Trainer Says:** Some patient chart holders have locks for keeping the patient charts secure. Your organization may want to use these in highly sensitive settings, such as psychiatric or substance abuse treatment areas.

**Rule #7: Avoid Leaving PHI Visible on Desktops or Work Surfaces**

Don’t leave visual PHI faceup on desktops or work surfaces (such as counters) for any longer than necessary, advises HIPAA consultant Errick Woosley. You should instead close file folders and turn over documents you’re working on, so that PHI isn’t visible to those not authorized to see it (like cleaning staff, patients, and visitors).
For the same reason, you should also clean off your desktop and work surfaces at the end of each shift or workday, Woosley recommends. He says you should then store the PHI in a secure area (see Rule #8). In some organizations, such as health care plans, this isn’t too significant an issue, because there’s minimal public traffic, says HIPAA security consultant Chris Apgar. For example, many health care plans have secure areas accessible only to authorized personnel.

**Rule #8: Store PHI in Secure Location**

Store documents and files containing PHI in secure locations, such as locked rooms, lockable storage bins, or lockable desk drawers. It’s also a good idea to store PHI in a secure location when you’ll be away from your desk or workstation for an extended period—say, more than 30 minutes—or if you’ll be leaving the premises during the workday, adds HIPAA expert Ann Geyer. If lockable storage isn’t available, keep PHI out of view and filed away—say, in closed desk drawers or filing cabinets—she adds (see Rule #7).

**Rule #9: Shred or Securely Dispose of Documents Containing PHI When No Longer Needed**

Shred or securely dispose of documents containing PHI when they’re no longer needed, recommends Brandt. This will protect PHI from falling into the hands of “Dumpster divers”—people who snoop through garbage looking for private information. Any PHI that goes into a Dumpster intact is at risk. If that happens, patients can sue your organization for leaving their PHI in a place where a Dumpster diver could get at it, and can file complaints with OCR saying you violated the HIPAA security or privacy regulations.

**Rule #10: Destroy Nonpaper Materials Containing PHI When No Longer Needed**

Similarly, don’t just dispose of nonpaper materials that contain PHI—such as plastic labels, prescription vials, transfusion bags, and damaged computer diskettes. Destroy them. These items are harder to destroy than paper, but they often contain even more PHI, says Berkeyheiser. For example, a used prescription vial may contain the patient’s name, prescribing physician, and the drug prescribed. And getting a look at the drug prescribed can give a snooper a good idea of the patient’s diagnosis.

To reduce this risk, strip these items of PHI before you dispose of them, suggests Berkeyheiser. For example, you can remove and destroy labels, disassemble and cut up diskettes, and hand-shred IV bags. Someone in your organization will tell you how to dispose of these items.

**Rule #11: If Possible, Use Separate, Locked Containers for Items Waiting to Be Shredded or Destroyed**

Usually you won’t be able to destroy items containing PHI right away. In fact, many health care organizations use an outside shredding or document destruction service to destroy materials. In the meantime, keep them under lock and key—preferably in locked bins or garbage cans, says Brandt.

She cautions that at one health care organization, a frugal volunteer tore the surgery schedule (which contained patients’ PHI) into quarters at the end of each day to give to visitors who asked for scratch paper.

Some organizations find that it hampers workflow to lock up paper with PHI on it, says Apgar. This is especially true for organizations with a large volume of paper. As an alternative for these organizations, he suggests using separate recycle bins. For example, each workstation might have a closed recycle bin for PHI, and that PHI might be collected nightly and placed in a larger, confidential recycling bin in a secure location.

**Rule #12: Ensure PHI on Computer Screens Isn’t Visible to Unauthorized Persons**

If you’re using a computer to store or access PHI, adopt safeguards to ensure that unauthorized persons won’t see PHI displayed on the computer screen. For instance, arrange your workspace so computer screens aren’t in the line of sight from doorways, windows, or aisles where visitors and passersby can easily view them.

Sometimes a computer screen can’t be moved where unauthorized persons won’t see it. In that case, a screen cover is a good security option, says Geyer. It’s a simple device that’s physically placed over the computer screen and left there at all times. It distorts or shades the screen for anyone looking at it from an angle, but doesn’t affect the view of a user who’s directly in front of the screen. But you shouldn’t rely solely on a screen cover if your desk is in a high traffic area, cautions Apgar. He notes that screen covers don’t work well when someone is standing directly behind the user. (For more information on safeguarding the security and privacy of patients’ PHI at computer
workstations, see “Safeguarding Workstations from Unauthorized Access to Patients’ PHI,” Trainer, Dec. 2003.)

Rule #13: Locate Fax Machines, Copiers, Printers, Scanners in Secure, Limited Access Areas

Often documents containing PHI can be found on fax machines, copiers, printers, and scanners. To protect PHI from being seen by unauthorized individuals, locate these machines in secure areas that are protected from unauthorized access and shielded from view. Ideally, a security key or I.D. badge, or some similar mechanism, should be required to gain access to fax machines, copiers, printers, and scanners used for documents containing PHI, suggests health care attorney Steve Fox, a partner at Pepper Hamilton LLP. But this may not be feasible in all organizations, notes Apgar. For example, a medical management unit isn’t likely to lock up a heavily used fax machine, because that would adversely impact workflow and patient care, he says.

Example: All fax machines, copiers, printers, and scanners used to send and receive PHI at XYZ Hospital are located in offices that are behind locked doors (such as its billing office and medical records department). Security keys to these departments are distributed only to employees authorized by their job descriptions to access and send PHI.

Example: ABC Laboratory has two fax machines, two copiers, and one computer printer. One fax machine and one copier are located in the reception area and used for administrative purposes. The second machine and copier, and the printer are located in a back office that’s inaccessible to patients and used for documents containing patients’ PHI.

For added security, don’t leave machines unattended when using them to print, send, or receive patients’ PHI, says Apgar. And promptly remove paper copies from fax machines, copiers, printers, or scanners, storing them in a secure place (say, a locked filing cabinet) (see Rule #8). Don’t leave paper copies of PHI where they might be viewed by unauthorized people (like on a desk), adds Berkeyheiser (see Rule #7).
ment area. The escort can also ensure that the representa-
tive doesn’t stray into areas where he doesn’t belong.

Berkeyheiser recommends making an exception to the
escort policy for visitors who arrive with or are assisting
patients. She says that visitors who accompany patients—
such as an adult child accompanying an elderly parent—
should be permitted in patient care areas without
supervision, if it’s okay with the patient.

Similarly, visitors who are in your facility to visit in-
patients generally don’t need to be escorted, says Berkey-
heiser. Instead, give passes to each visitor. Visitors’ passes
should be visible from a distance to make it easier for staff
to quickly identify and redirect visitors who aren’t where
they belong. For example, if an employee sees a visitor
looking at a patient chart left on a counter, the employee
could quickly pick up the chart and remove it from the
visitor’s view. The employee could then ask the visitor
whether he needs help locating a particular floor, wing,
or department of your facility.

TRAINER SOURCES
Chris Apgar, CISSP: President, Apgar & Assocs., LLC, 10730 SW
62nd Pl., Portland, OR 97219; capgar@easystreet.com.
Lesley Berkeyheiser: Principal, The Clayton Group, 53 Bethel Rd.,
Glen Mills, PA 19342; lberkeyheiser@theclaytongroup.org.
Mary D. Brandt, MBA, RHIA, CHE, CHPS: President, Brandt &
Assocs., Inc., 4610 Braeburn, Bellaire, TX 77401; mbrandt@brandt
associates.com.
Steven J. Fox, Esq.: Pepper Hamilton LLP, 600 14th St. NW, Ste.
500, Washington, DC 20005.
Ann Geyer: Partner, Health Care Practice, Tunitas Group, PO Box
278, Mountain Ranch, CA 95248; ageyer@tunitas.com.
Tom Hanks: Partner, Health Care Strategy & Change, IBM Business
Consulting Services, One IBM Piz., Chicago, IL 60611;
TomHanks@us.ibm.com.
Errick Woosley: Coadunate Consulting, LLC, 2067 Rock Creek Rd.,
Batesville, IN 47006; woosleew@aol.com.

TRAINER’S QUIZ

We’ve given you an overview of what you must do to safeguard PHI to minimize the risk that visual PHI
will be seen by those not authorized to see it. Now let’s see if you can apply these 14 rules to real-life situa-
tions that health care organizations like yours are likely to encounter. The TRAINER’s Quiz, below, will
give you an opportunity to test your knowledge. Take it, and see how well you do.

INSTRUCTIONS: Analyze the questions below according to the 14 rules we’ve given you for safeguarding
visual PHI. Circle the answer you think is right. The correct answers (with explanations) appear after the
quiz. Good luck!

QUESTION #1
Patient A is treated at XYZ Cardiology Associates. Nurse X
places Patient A's chart in a chart holder outside the exam
room. True or false: XYZ Cardiology Associates must use
a locking chart holder to safeguard Patient A's privacy?
a. True.
b. False.

QUESTION #2
XYZ Hospital requires all employees in its billing depart-
ment to shred all documents containing PHI when no
longer needed. Employee A gets a phone call and takes
a billing report out of the “to be shredded” container.
She uses the back of the discarded billing report for
scratch paper. The billing report lists patients’ names,
addresses, and insurance information. Did Employee A
do anything wrong?
a. Yes.
b. No.

QUESTION #3
Baby A is born at XYZ Hospital. Baby A’s parents give a
picture of Baby A to Employee X. Employee X posts a
picture of the new baby on a maternity ward bulletin
board, after getting written authorization from Baby A’s
parents to do so. Did Employee X do anything wrong?
a. Yes.
b. No.

© 2004 by Brownstone Publishers, Inc. Any reproduction is strictly prohibited. Copying training program materials is a violation of federal law.
To subscribe, call 1-800-643-8095 or visit www.brownstone.com
**TRAINER’S QUIZ**

**QUESTION #4**
Patient A goes to XYZ Medical Group for her yearly exam. The receptionist says, “Patient A, please include your age, address, Social Security number, reason for today’s visit, and phone number on the sign-in sheet.” Did the receptionist do anything wrong?

a. Yes.
b. No.

**QUESTION #5**
Employee A’s workstation is located in an area that’s accessible to the general public. She’s working on documents containing Patient P’s PHI. At the end of the workday, she closes Patient P’s file and leaves it on her desk so she can finish it in the morning. Did Employee A do anything wrong?

a. Yes.
b. No.

---

**TRAINER’S ANSWERS & EXPLANATIONS**

**QUESTION #1**
Correct answer: b

Reason: Rule #6 applies here:

Rule #6: If You Must Leave Patient Chart in Holder Outside Exam Room, Keep It Covered or Turned Around

The HIPAA privacy regulations don’t require a health care organization (like XYZ Cardiology Associates here) to use locking chart holders to safeguard a patient’s privacy when using chart holders. However, it’s a good idea to keep the chart either covered or turned around in the chart holder.

Wrong answer explained:

a. As explained above, the HIPAA privacy regulations don’t require the use of locking chart holders to safeguard a patient’s PHI.

**QUESTION #2**
Correct answer: a

Reason: Rules #9 and #11 apply here:

Rule #9: Shred or Securely Dispose of Documents Containing PHI When No Longer Needed

Rule #11: If Possible, Use Separate, Locked Containers for Items Waiting to Be Shredded or Destroyed

Employee A should have shredded the billing documents containing PHI when they were no longer needed. If she wasn’t able to destroy items containing PHI right away, she should have kept them under lock and key—preferably in locking bins or garbage cans. She shouldn’t have used documents containing PHI for scratch paper.

Wrong answer explained:

b. As explained above, Employee A should have either immediately shredded the documents containing PHI, or placed them in a locking container for later destruction.

**QUESTION #3**
Correct answer: b

Reason: Rule #3 applies here:

Rule #3: Get Patient’s Written Authorization Before Posting Cards, Letters, or Photos

To safeguard Baby A’s privacy, Employee X properly got Baby A’s parents to sign an authorization before she posted Baby A’s picture on XYZ Hospital’s bulletin board.

Wrong answer explained:

a. As explained above, Employee X properly got an authorization to post Baby A’s picture on a hospital bulletin board.
QUESTION #4
Correct answer: a
Reason: Rule #1 applies here:

Rule #1: Limit PHI Written on Sign-In Sheets
A health care provider (like XYZ Medical Group here) may use a sign-in sheet. But if it does so, it must make reasonable efforts to safeguard the patient’s privacy by limiting the amount and type of PHI it asks for. Here, the receptionist didn’t simply ask the patient to write her name and time of arrival on the sign-in sheet. Instead, the receptionist asked the patient to write her age, address, Social Security number, phone number, and reason for visiting on the sign-in sheet—PHI that wasn’t needed for sign-in purposes.

Wrong answer explained:
b. The receptionist should have made reasonable efforts to safeguard Patient A’s privacy by limiting the amount of PHI she asked for.

QUESTION #5
Correct answer: a
Reason: Rules #7 and #8 apply here:

Rule #7: Avoid Leaving PHI Visible on Desktops or Work Surfaces
Rule #8: Store PHI in Secure Location
To safeguard Patient P’s privacy, Employee A should have cleaned off her desktop at the end of her workday and removed Patient P’s file. She should then have stored Patient P’s file in a secure location (like a locked filing cabinet). If lockable storage wasn’t available, Employee A should have stored the file somewhere out of view—for example, in her desk drawer.

Wrong answer explained:
b. Employee A should have made reasonable efforts to safeguard Patient P’s privacy by storing the file in a secure location at the end of her workday.