Understanding the Privacy and Security Regulations

HIPAA Handbook for Healthcare Staff

HCPro
## CONTENTS

About the Expert ........................................................................................................ vi

Intended Audience ..................................................................................................... 1

Learning Objectives ................................................................................................. 2

HIPAA Basics ........................................................................................................... 2

- HITECH Act overview ............................................................................................ 3
- HIPAA and you ....................................................................................................... 3

Terms You Should Know .......................................................................................... 3

- Covered entities ..................................................................................................... 3
- PHI .......................................................................................................................... 4
- Treatment, payment, and healthcare operations .................................................. 6
- Minimum necessary/need to know ......................................................................... 6
- Case scenario #1: Celebrity sighting ...................................................................... 8

Privacy ......................................................................................................................... 9

- What your facility does to protect confidentiality ................................................. 10
- What you can do to protect confidentiality ............................................................. 10
- Case scenario #2: Family members and PHI ......................................................... 11
- Case scenario #3: Good intentions ........................................................................ 12
- Case scenario #4: Sometimes you need to vent .................................................... 13
- Faxing ..................................................................................................................... 13
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case scenario #5: “Hello, Pete’s Plumbing, how may I help you?”</td>
<td>14</td>
</tr>
<tr>
<td>Discarded patient information</td>
<td>15</td>
</tr>
<tr>
<td>Patient directory</td>
<td>15</td>
</tr>
<tr>
<td>Incidental disclosures</td>
<td>16</td>
</tr>
<tr>
<td>High-risk situations: Elevators, lobbies, and other public places</td>
<td>16</td>
</tr>
<tr>
<td>High-risk situations: Printouts</td>
<td>17</td>
</tr>
<tr>
<td>High-risk situations: Friends and family</td>
<td>17</td>
</tr>
<tr>
<td>Case scenario #6: Mum’s the word</td>
<td>17</td>
</tr>
<tr>
<td>Helping Patients Understand Their Rights</td>
<td>18</td>
</tr>
<tr>
<td>Notice of privacy practices</td>
<td>18</td>
</tr>
<tr>
<td>Security</td>
<td>20</td>
</tr>
<tr>
<td>Security: What you can do</td>
<td>21</td>
</tr>
<tr>
<td>Security: What your facility does</td>
<td>21</td>
</tr>
<tr>
<td>Passwords and personal user IDs</td>
<td>22</td>
</tr>
<tr>
<td>Tips and tricks to protect your password</td>
<td>22</td>
</tr>
<tr>
<td>Sharing passwords</td>
<td>23</td>
</tr>
<tr>
<td>Protecting against computer viruses</td>
<td>25</td>
</tr>
<tr>
<td>Unauthorized software</td>
<td>25</td>
</tr>
<tr>
<td>Unauthorized hardware</td>
<td>26</td>
</tr>
<tr>
<td>E-mail security</td>
<td>26</td>
</tr>
<tr>
<td>Encryption</td>
<td>27</td>
</tr>
<tr>
<td>Protecting hand-held devices and laptop computers</td>
<td>27</td>
</tr>
<tr>
<td>What you can do to protect physical security</td>
<td>28</td>
</tr>
</tbody>
</table>
Kate Borten, CISSP, CISM

Kate Borten, president of The Marblehead Group in Marblehead, MA, brings clients a unique combination of expertise in information security, privacy, and IT from more than 20 years in the healthcare industry. She was chief information security officer at Beth Israel Deaconess Medical Center in Boston and led the first corporatewide security program at Massachusetts General Hospital.

Borten is a nationally recognized expert on HIPAA and health information privacy and security and a frequent speaker on the topic. She is the author of several HIPAA publications, including The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit (HCPro, Inc., 2007) and The HIPAA and HITECH Toolkit: A Business Associate and Covered Entity Guide to Privacy and Security (HCPro, Inc., 2009), and a contributor to privacy and security newsletters.

The Marblehead Group (http://marbleheadgroup.com) provides HIPAA privacy and security assessment, compliance auditing, and solutions to health plans, business associates, and the full range of provider organizations.
HIPAA Handbook for Healthcare Staff

Understanding the Privacy and Security Regulations

Intended Audience

This book explains the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules as applicable and relevant to a healthcare organization’s general work force. It also addresses the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 privacy and security provisions. The intended audience includes:

- Clerical staff, including medical records staff, patient accounting and registration, back office staff, and HR
- Nutrition services staff
- Nursing assistants
- Housekeeping/facilities staff
- Trainees/students and volunteers
- All other ancillary staff
Learning Objectives

This book explains certain HIPAA and HITECH Act requirements for privacy and security. It covers workplace practices that protect patient privacy and ensure the security of confidential health information. After reading this book, you should be able to:

- Describe the HIPAA and HITECH Act privacy and security requirements for covered entities
- Define protected health information (PHI) and explain why protecting patient privacy is important
- Summarize how to protect confidential health information by following proper physical security procedures
- Describe how to protect confidential information you may come across while performing your job
- Contact the correct individual with your questions about protecting patient privacy
- Be prepared to help prevent identity theft in your organization

HIPAA Basics

HIPAA is a federal law that protects the privacy of patients and all information about them. HIPAA gives patients the right to have their information kept private and secure. It is more than just a good idea—it is a federal law with penalties (even criminal ones) for violations.
**HITECH Act overview**

The American Recovery and Reinvestment Act of 2009 (ARRA) became federal law February 17, 2009. A subset of the ARRA is called the HITECH Act, which, among other goals, enhances and expands the HIPAA Privacy and Security Rules. The HITECH Act not only makes privacy regulations more strict, but it gives more power to federal and state authorities to enforce privacy and security protections for patient data.

**HIPAA and you**

Regardless of your position in the organization, you have constant access to PHI and may regularly communicate with patients and their families and friends, as well as your colleagues. So understanding what HIPAA requires with respect to privacy and security is particularly important for you. No matter where you work in healthcare—a hospital, laboratory, radiology center, nursing home, or office—you must understand what HIPAA requires of you to keep patient information, in any form (e.g., written, verbal, or electronic), private and secure.

**Terms You Should Know**

You may hear the following terms mentioned when discussing HIPAA:

**Covered entities**

HIPAA Privacy and Security Rules apply to all “covered entities.” Covered entities include health plans, healthcare clearinghouses, and most provider organizations, such as physician practices, therapists,
dentists, hospitals, ambulatory facilities, nursing homes, home health agencies, and pharmacies. Your employer is a covered entity. All HIPAA covered entities must comply with the Privacy and Security Rules, as well as the enhanced privacy and security provisions of the HITECH Act.

**PHI**

HIPAA protects patient health information. Protected health information is known as PHI. HIPAA establishes rules for when and how healthcare staff members may use or release patients’ PHI.

PHI includes any information that can be used to identify a patient. It can be:
PHI includes demographic information (e.g., person's name), financial information (e.g., insurance and billing), and health information (e.g., diagnosis codes).

### These are typical identifiers

<table>
<thead>
<tr>
<th>PHI</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Maria A. Miller</td>
</tr>
<tr>
<td>Address</td>
<td>123 Main Street, Millersville, MA 01234</td>
</tr>
<tr>
<td>Employer</td>
<td>Millersville Museum of Art</td>
</tr>
<tr>
<td>Relatives' names</td>
<td>Thomas Miller, husband</td>
</tr>
<tr>
<td>Date of birth</td>
<td>7/21/80</td>
</tr>
<tr>
<td>Telephone number</td>
<td>987/654-3210</td>
</tr>
<tr>
<td>E-mail address</td>
<td><a href="mailto:iluvhipaa@hotmail.com">iluvhipaa@hotmail.com</a></td>
</tr>
<tr>
<td>Social Security number</td>
<td>123-45-6789</td>
</tr>
<tr>
<td>Medical record number</td>
<td>#1123581321</td>
</tr>
<tr>
<td>Member or account number</td>
<td>#357111317192329</td>
</tr>
<tr>
<td>Fingerprints</td>
<td></td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Characteristics (e.g., job) that could identify someone</td>
<td>Museum docent</td>
</tr>
</tbody>
</table>
PHI includes medical information

PHI includes medical or healthcare-related information if it can be tied to one specific patient, including:

- The reason a person is sick or in the hospital
- The treatments and medications he or she may receive
- Test results
- Observations about the patient’s condition
- Information about past health conditions or treatments
- Discharge planning information
- Billing information

Treatment, payment, and healthcare operations

HIPAA permits healthcare staff members to use and share PHI to perform their job for three reasons without patient permission:

- Treatment
- Payment
- Healthcare operations

Minimum necessary/need to know

Only staff members who “need to know” PHI to perform their jobs may have access to it. HIPAA requires healthcare workers to use or share
only the “minimum necessary” information to perform their jobs. Ask yourself the following questions before viewing any patient information:

- Do I need this information to perform my job?
- What is the least amount of information I need to perform my job?

Examples of using minimum necessary and need-to-know standards

If you work in food services, you may need to know dietary information about a particular patient to perform your job, but you probably don’t need to know other medical information about the patient to perform your job in food services. Therefore, do not look at other information about this patient or any information about other patients.

If you are a member of the front office or registration staff, you will come in contact with PHI as you register patients, deal with insurance matters, and interact with other healthcare providers. But you may access only the parts of the patient medical records that are necessary to perform your job and only the records of the patients you need to access to perform your job. Accessing additional information or other patients is a violation of HIPAA.

Or, perhaps you are a member of the housekeeping staff and you come across some discarded test results while you clean a room after a patient has been discharged. Don’t look at the information, because you
do not need to know the information. And if you recognize a patient’s name, you must keep this information to yourself.

**Case scenario #1: Celebrity sighting**

You walk into a patient’s room and are surprised to see the local news station’s meteorologist in the hospital bed. During your break in the cafeteria later that day, you ask other staff members if anyone knows why she is in the hospital. The three of you discuss whether her bleached-blonde hair could withstand the recent heavy winds. Your conversation seemed harmless because it was among staff members who all work at your facility. But something tells you it was inappropriate.

**Did you do anything wrong?**

Yes. You shouldn’t have revealed that the meteorologist was a patient. Discussing her was inappropriate because your coworkers may not have known she was a patient. And your conversation wasn’t for job-related purposes, it was just chitchat. Also, the conversation occurred in a very public area—a crowded cafeteria—something you should avoid if at all possible. This violated the woman’s privacy. You may use, disclose, or tell someone PHI only when it’s necessary to perform your job.

Otherwise, generally speaking, it is prohibited. Patients’ right to privacy has been violated in some well-publicized cases, such as when actor George Clooney received treatment after a motorcycle accident.
and when former President Bill Clinton underwent cardiac surgery. In both cases, staff members, including physicians, accessed the patient’s information, despite their lack of involvement in the patient’s care. Disciplinary action resulted in both cases.

**Testing Your Understanding**

**Which of the following pieces of information is permissible to share with a friend?**

a. A photo you took of the newly redecorated waiting room with a few patients sitting around.

b. The patient you cared for recently with a highly unusual set of symptoms

c. A completed charity care application

d. Statistics on cancer survival rates

**Best answer:**

d. A general trend is okay to discuss, but never refer to a specific patient’s conditions, diagnosis, or other medical information

**Privacy**

Patients receiving medical care expect privacy whether they are in the hospital, a physician’s office, a laboratory, or another healthcare setting. They expect to interact with caregivers away from the public whenever possible. They expect that caregivers will not share their PHI with individuals who don’t need to know it.
What your facility does to protect confidentiality

Your facility protects confidentiality by:

- Locking records and allowing access only to those individuals who need information for treatment, payment, healthcare operations (commonly referred to as TPO), or other authorized purposes
- Requiring employees and others with computer access to patient records to log off their computers while they are away from their desks
- Turning computer screens away from public view or using privacy screens to ensure that information is not accessed accidentally
- Monitoring access to electronic records by maintaining and reviewing audit trails to ensure that they are being used appropriately
- Cross-shredding any paper that includes PHI before discarding it
- Educating all staff members with respect to privacy and security policies
- Requiring all staff members to commit in writing to maintaining the privacy and security of PHI (preferably annually)

What you can do to protect confidentiality

Use these tips to help protect privacy:

- Avoid discussions about patients in elevators and cafeteria lines, at nurses’ stations, and other public places, both inside and outside the organization.
• Return paper patient information to its appropriate location or properly destroy it when you are done using it.

• Be aware of HIPAA’s privacy regulations if your children or other guests accompany you to work. Your guests should not be able to see PHI in any form.

• Don’t discuss patients with anyone except when necessary for work-related purposes.

• Don’t share information that you accidentally overhear or see with anyone who doesn’t need to know the information to perform his or her job.

• Don’t discuss a patient’s condition or treatment with family members or other visitors. Instead, politely refer these people to the clinical staff member who can respond to their questions appropriately.

Case scenario #2: Family members and PHI

A patient asks the hospital to not disclose her PHI to her brother. She submits the request in writing, and the facility agrees. Later, the patient is admitted to the hospital with end-stage renal failure. Her brother visits the hospital and asks a nurse for an update on his sister’s condition.

What, if any, PHI can the nurse disclose?

None. When a patient asks your organization not to give out PHI to a particular family member and your organization
agrees, you cannot disclose PHI to that family member in any form, at any time.

**Case scenario #3: Good intentions**

A lab worker receives a specimen labeled with the name of someone he knows from church. From the test that’s been ordered, he has an idea of the patient’s medical problem. He then calls other members of the church who put the information out on a prayer chain. Suddenly, several hundred people know of the person’s illness.

**Is this an acceptable disclosure?**

No. If you look at patient records for any nonbusiness reason, even if it’s with the best intentions, it is cause for dismissal and possible legal consequences. Likewise, if you look at the records for the right reasons, but pass the information along to others who don’t have a right to know, you are also violating your organization’s policy and the law.

Remember that this rule applies to everyone in your organization, including employees, doctors, nurses, and volunteers. If doctors or nurses look at confidential information about patients for nontreatment purposes, they can be fired or lose their privileges to work at the hospital.

If doctors or nurses share information about patients outside the hospital with people who do not have a right to know that information,
they can be fired or lose their privileges to work at the hospital. Further, there may be legal consequences and their licenses may be in jeopardy.

**Case scenario #4: Sometimes you need to vent**

You chat with another staff member as you leave for the day and decide to go out for dinner before going home. During dinner, you find yourselves venting about work. This includes a discussion about a difficult patient. You are careful never to mention the patient’s name as you describe the situation to your colleague.

**As you drive home after dinner, you wonder whether you said too much. Did you?**

You were correct not to mention the patient’s name. However, you must remember that sharing too many details about a patient to colleagues could enable them to know who you’re discussing. Don’t share PHI with anyone—including family members, friends, or other staff members—who doesn’t need to know the information. You must resist the temptation to share stories—no matter how interesting—with colleagues, friends, and family members who don’t need to know, even if you omit the patient’s name.

**Faxing**

HIPAA does not address faxing patient information specifically, but it does protect faxed information under the Privacy Rule. Remember that faxed patient information can easily fall into the wrong hands, which would be a privacy violation. Faxing is actually a very risky way
to transmit PHI because dialing a number incorrectly is so easy to do. Before faxing any patient information, be certain that you know your facility’s fax policy and any limits on its use. Use these tips when faxing to help protect confidentiality:

- Use a cover page with a confidentiality message.
- Verify the number to which you are faxing. Ensure that you are sending a fax to the correct person at the correct number.
- Confirm with the recipient that you are sending the correspondence to a dedicated fax machine in a secure location.
- Ensure that the person to whom the information is faxed is authorized to receive the information.
- Call to confirm that the person received the fax.
- Before receiving a fax, ask the sender to notify you beforehand so that you can be present to receive the fax.
- Remove pages from the fax machine immediately upon receipt.

Case scenario #5: “Hello, Pete’s Plumbing, how may I help you?”

At a patient’s request, you fax some test results to her primary care physician’s office. You include a cover page that describes the information as confidential. You receive a call approximately 20 minutes
Later. You accidentally faxed the patient’s information to Pete’s Plumbing, a small business in Oklahoma.

**What should you do?**

Ask the caller to destroy the records. Inform your manager about the mistake and follow any additional protocols at your organization for dealing with an accidental privacy breach. In the future, double-check fax numbers beforehand. Consider using your fax machine’s speed dial feature for frequently dialed fax numbers to eliminate the chance of misdialing in the future.

Luckily, Pete was a nice guy. Imagine the aftermath if you’d sent hundreds of people’s information to a huge company with 1,000 employees. You could have a massive privacy breach.

**Discarded patient information**

Don’t discard patient information in a trash receptacle without shredding it or following your organization’s procedures for destroying confidential information. The receptacle could tip over or the contents could fall off a recycling truck and blow down the street. If you come across PHI in a trash receptacle or discarded in some other way, notify your supervisor to ensure its proper disposal.

**Patient directory**

A patient directory is a list of patients within a facility. It provides certain information to people, including visiting clergy, family, or friends.
who ask for a patient by name. HIPAA permits directories to include patients’ names, location, and general condition. Patients who so desire may be excluded from the directory. If visitors request information about a patient, direct them to the information desk for assistance. Even if you just want to be helpful, if it’s not your job you may accidentally give out information you shouldn’t.

**Incidental disclosures**

Sometimes you may have incidental access to confidential information. For example, you may overhear a physician speaking to a patient about her diagnosis or you may hear therapists discussing a patient’s treatment plan. This is PHI that must be kept confidential, so you should not share this information with anyone else.

**High-risk situations: Elevators, lobbies, and other public places**

High-risk areas where you might be tempted to discuss a patient, probably without realizing the risks associated with doing so, include elevators, lobbies, and other public places. Remember that these are places and situations where discussion of PHI is inappropriate.

Elevators might seem to be a convenient place to converse as you go from floor to floor, but it is probably impossible for other passengers to avoid eavesdropping. Try to avoid discussing patients in lobbies and other public places, such as cafeterias; keep your voice low or move to a private place if at all possible.
**High-risk situations: Printouts**

Do not leave printed information strewn about. File or dispose of it properly when you are done using it. Never take PHI outside your facility unless you have specific permission from your supervisor or privacy officer.

**High-risk situations: Friends and family**

HIPAA requires hospitals and other healthcare providers to obtain permission from patients before sharing PHI with their family members or friends. Be careful not to provide patients’ families and friends with any information you may have learned while performing your job. If patients or their families or friends ask you to do so, alert a nurse or other staff member involved in their care so that he or she can assist them.

You may not view your family’s or friends’ medical records unless you need to know the information to perform your job or unless the patient has given your facility permission for you to do so. Otherwise, viewing these records violates HIPAA. Notify your supervisor if circumstances put you in the position of handling PHI for a family or friend.

**Case scenario #6: Mum’s the word**

You notice on the patient directory list the name of a patient who is a longtime friend of your mother. During a break, you go to her room and chat with her briefly before returning to work. You are careful not to inquire about the reason for her hospitalization. Later that evening, you call your mother to tell her that you saw the friend.
Did you do anything wrong?

Chatting with the patient is permissible, as long as she initiates the conversation. Let her take the lead. She may not be interested in chatting. But you absolutely should not tell your mother that you saw her friend unless the patient tells you to let your mother know. Sharing information you learn at work with people outside of the hospital is a HIPAA violation. The patient may not want others to know she is hospitalized. Telling your mom you saw the patient violates her friend’s privacy. You should not share patient information with anyone who doesn’t need to know it. This includes your family and friends.

Helping Patients Understand Their Rights

Patients must understand how providers may use and disclose their information.

Notice of privacy practices

The HIPAA Privacy Rule requires healthcare providers to hand out and post a privacy notice telling patients all the ways in which their information can be used and released to another organization or to the government.

This notice of privacy practices also tells patients about their rights under HIPAA, including the right to view their own records, obtain copies, and request amendments to them. The privacy notice must also
let patients know how to file a complaint with your organization or with the U.S. Department of Health and Human Services.

Because this privacy notice is so important, HIPAA requires providers to make a good faith effort to obtain each patient’s written acknowledgment that he or she received a copy of the notice of privacy practices.

You will also see these information notices posted in places where patients can see them. If patients have questions about how the organization uses information, you can direct them to these posted notices or to the organization’s privacy official for answers.

Exceptions to the rules

Your organization may be permitted or required by other laws and regulations to release patient information without first asking the patient to agree or authorize the disclosure.

Always be sure you know your organization’s policies before releasing information and check that the particular instance is approved.

The following are examples of scenarios in which your organization may be subject to laws and regulations permitting or requiring release of patient information:

- Releasing information about the patient’s location in a facility (however, the patient has the right to opt out of the facility directory listing)
• Reporting certain information to public health agencies

• Reporting certain information about medical devices that break or malfunction to the FDA

• Reporting suspected child abuse or domestic violence to the police or state child welfare agency

• Responding to court orders

• Reporting cases of suspicious deaths or suspected crime victims

• Responding to certain requests from the military

**Understanding your role**

In all of these cases, the facility complies with the law and makes reports when necessary. Unless reporting this information is part of your job, do not report this information yourself. If you are interested in more information about what your state requires, contact your facility’s privacy official. That person can, if needed, check with legal counsel or the attorney general.

**Security**

HIPAA requires security protections for all forms of PHI, not just electronic.
Security: What you can do

Your facility’s information security officer has ultimate responsibility for information security policies in place at your facility. However, everyone has an important role to play in keeping information secure by following policies and procedures. The technical, physical, and policy safeguards your organization has implemented to secure patient health information are useless without the cooperation of everyone who works at the facility. Properly managing your password, preventing the spread of viruses, logging off your computer, and being aware of and responsible for any patient information taken or accessed off-site are important ways you can contribute to information security.

Note: Every facility must have a designated privacy and security officer. These can be different persons or the same individual.

Security: What your facility does

Your facility ensures security by:

- Monitoring logon attempts
- Responding to information security incidents
- Employing appropriate measures to protect computers from viruses and malicious software
- Protecting patient information that is removed from the facility or accessed from home
- Educating staff members about security practices
HIPAA Handbook for Healthcare Staff

- Conducting random security audits to ensure that only staff members who need to know are accessing PHI, and that they are accessing only the minimum records necessary to perform their jobs
- Using appropriate physical security measures such as door locks
- Implementing data recovery plans and downtime procedures
- Implementing “role-based access” so that staff members access only the information they need to perform their jobs

Passwords and personal user IDs

Organizations need to know who views and updates what information. Everyone has his or her own unique user ID (logon ID or logon name) and password, so that computer systems can track activity back to each user. Although it may seem convenient to do so, you must never let other people “borrow” your ID and password to log on to the computer system. This is a security violation, and you will be held responsible for the other person’s computer activity. And don’t ask others whether you can use their IDs and passwords.

Tips and tricks to protect your password

Selecting a strong computer password—one that is easy for you to remember but difficult for someone else to guess—is an essential step in securing your organization’s information. Generally, you should select a password that:

- Includes both letters and numbers
• Consists of at least six characters (your organization may require seven or eight)

• Incorporates upper- and lowercase letters if your system is capable of supporting them

• Includes special keyboard characters (such as #) if your system permits

• Isn’t a personal name, special date, fictional character, or real word

**Note:** Change your password regularly, at least once every 90 days or whenever you suspect someone has learned your password. Don’t repeat a password or use a very similar one for at least five password changes.

**Sharing passwords**

No one but you should know your password. If a coworker requests your password, refer that individual to your manager or your organization’s help desk or technical support department so that he or she can obtain appropriate access to the necessary information. If you share your password—even if you think it is for a good reason—you are violating security policy.

In addition to creating a security problem, using someone else’s access may also interfere with performing your job. Your user ID and password are set up specifically to allow you access to the information you
need for your job. Someone else’s credentials may not give you access to the information you need.

**Testing Your Understanding**

It’s been a few months since Jennifer Jones, a coder based in Atlanta, has changed her computer password, and she thinks it is time to do so. She is pretty sure her old password, “jjones,” could be better. In fact, she wants to make her new password as secure as possible.

Which of the following is her best choice?

- a. JjOnEs. She added some odd capitalization to make it harder to guess.
- b. JJ!Atlan98. She combined numbers, letters, the year she moved to Atlanta, even a special character, but it’s still catchy.
- c. jj0ne5. She changed the O to a zero, and the S to a five. How clever!
- d. JenJ. She made it different but still easy for her busy brain to remember.

**Best answer:**

b. This combines numbers, upper- and lowercase letters, and a special character (the exclamation point), and it isn’t based solely on her name.
Protecting against computer viruses

A computer virus or other malicious software can destroy information stored on your computer. And it can copy your passwords or PHI that you store or send. Viruses often are transmitted via e-mail attachments or by visiting certain Web sites.

Dos and don’ts for protecting against viruses

<table>
<thead>
<tr>
<th>Dos</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tell your IT department if you receive an unrecognizable or suspicious e-mail or an unfamiliar program appears on your computer.</td>
<td>Don’t open suspicious e-mail and attachments from unrecognized senders.</td>
</tr>
<tr>
<td>Follow your organization’s policy for using antivirus software and keep it up to date.</td>
<td>Don’t uninstall any antivirus applications installed on your computer.</td>
</tr>
<tr>
<td>Use your e-mail in a manner that is consistent with your facility’s policies and procedures.</td>
<td>Don’t access unapproved personal e-mail accounts while you are at work. (Web-based e-mail, such as Hotmail® and Gmail™, is convenient, but you should use it only if your department approves.)</td>
</tr>
</tbody>
</table>

Unauthorized software

Music-sharing and remote-access software, games, and other programs that you may want to install can disable your computer, threaten your organization’s network, and contain malicious software that would allow someone to access your computer.
Don’t install any software on your computer without permission from your IT department. Make special note of file types before opening them. Files that end with “.exe” are executable files, or software programs. Viruses or malicious software programs often are contained in downloaded executable files. Do not open these files without permission from your technical support department.

**Unauthorized hardware**

Use similar precautions when installing hardware. Any device attached to your organization’s network or your computer must be installed with the appropriate security precautions in mind.

For that reason, you should connect other devices, such as computers and servers, to the network only if you have received permission to do so from your technical support staff. And you should connect devices to your computer—for example, through the USB port—only with permission from the technical support department.

**E-mail security**

Information that you e-mail is usually not secure. For that reason, your organization has adopted strict policies with regard to how it electronically transmits PHI. Your organization’s e-mail program may encrypt information before sending it, or you may have special Web-based tools for transmitting patient information. Some organizations ban the inclusion of PHI in e-mail.
Remember that even if the technology works, e-mail, like faxing, is subject to misdirection. Also, organizations that send PHI via e-mail may need to determine how to store it or may need to print and file it in the patient’s record because it becomes part of the legal record. Before you transmit PHI in electronic form, ensure that you comply with your organization’s policies.

**Encryption**

Encryption simply means that information is coded or scrambled so that it cannot be read by anyone who doesn’t have the key to read it. Many organizations encrypt the data they store or transmit depending on whether there is a high risk that the information might be read by an unauthorized individual.

For example, PHI sent via the Internet or stored on portable computers (e.g., laptop computers, or hand-held devices) and disks is at a higher-than-average security risk. Many organizations now require encryption in these circumstances. Often, software programs that encrypt data operate invisibly to users. You need to know whether your organization requires that you take steps to encrypt data.

**Protecting hand-held devices and laptop computers**

Many healthcare workers use hand-held devices and laptop computers, and the most frequent risk when doing so is the risk of loss or theft of the device. This results in a loss of equipment and potential loss of data confidentiality. Lock devices in a drawer or briefcase when not in use.
Use. If your device is stolen or lost, file an incident report with your facility as soon as possible.

Use these tips to protect hand-held devices and laptop computers:

- Do not save PHI on portable devices unless protected by a password. Do not store passwords and access codes on hand-held devices.
- Back up information stored on portable devices.
- Consider encrypting PHI on portable devices.
- Pay special attention to portable media (e.g., disks, CDs, and thumb drives) that you take off-site.
- Secure portable devices in a locked area or receptacle when not in use.

**What you can do to protect physical security**

Even if you don’t have access to computers while you work, you can still help your facility protect security.

Use these tips to help protect physical security:

- Do not use a computer unless you have authorization to do so and you have received your own user ID (sometimes called username or login ID)
• If you need to use a computer to perform your job, keep your computer screen turned away from public areas or use a privacy screen. Log off the computer when you are done.

• If you see disks or CDs that may have PHI on them strewn about, give them to your supervisor.

• If you work with printed PHI, don’t leave this information strewn about.

• Shred paper or follow your hospital’s procedures for destroying patient information before discarding it.

• If you see unprotected PHI as you perform your job, do not look at it; instead, notify the nearest supervisor.
The Federal Trade Commission (FTC) created the Red Flags Rule to protect consumers from identity theft by requiring “creditor” organizations to implement a formal identity theft program.

The FTC describes “creditor” as a business or organization that permits customers (including patients) to pay for products or services in multiple installments over time. This definition includes most
healthcare providers that permit deferred payment for services, even if only occasionally.

Red Flags are warnings that there may be identity theft occurring. The program must include appropriate red flags that, when triggered, lead to special organizational procedures. The rule includes many examples in categories such as suspicious documents; suspicious personally identifying information (e.g., driver’s license with a photograph that bears no resemblance to the person presenting it); and notices from patients who are victims of identity theft, law enforcement officials, or other businesses about possible identity theft involving an individual’s account.

If you suspect a patient is not the person he or she claims to be, immediately alert the privacy officer and/or security officer in your facility so that he or she may alert the proper authorities. Identity theft is serious, and medical identity theft, a special form of identity theft, can have financial and life-threatening consequences.

The Consequences of Breaking the Rules

Violating the HIPAA or HITECH Act’s Privacy or Security Rules can result in civil or criminal penalties. Pursuant to HIPAA, civil penalties currently include fines of up to $25,000 for repeated violations of a single requirement in a calendar year. However, with the HITECH Act, the fines become much higher. Criminal penalties for
wrongful disclosure of patient information can include not only large fines, but also incarceration. The criminal penalties increase as the severity of the offense increases.

For example, selling patient information is more serious than accidentally allowing its release, so it brings stiffer penalties. These penalties can be as high as a $250,000 fine or a prison sentence of 10 years.

Civil penalties

The civil penalties for a HIPAA or HITECH Act violation are based on the following tier system:

- **Tier A**: The offender did not know he or she violated the law. The fine is $100 for each violation, with a maximum fine of $25,000 for multiple violations of the same requirement or prohibition in one calendar year.

- **Tier B**: Violation due to reasonable cause, but not willful neglect. The fine is $1,000 for each violation, with a maximum fine of $100,000 for multiple violations of the same requirement or prohibition in one calendar year.

- **Tier C**: Violation due to willful neglect, but corrected within a required time period. The fine is $10,000 for each violation, with a maximum fine of $250,000 for multiple violations of the same requirement or prohibition in one calendar year.
• **Tier D**: Violation due to willful neglect, and the organization did not correct it. The fine is $50,000 for each violation, with a maximum fine of $1,500,000 for multiple violations of the same requirement or prohibition in one calendar year.

**Obtaining Help**

You may have a question about HIPAA or about how your hospital complies with other regulations. Don’t hesitate to contact your privacy or information security officer with questions. These individuals will be glad to answer your questions.

**Reporting Violations**

Your hospital needs all employees and volunteers to follow its privacy and security policies, but it realizes that some individuals may violate the rules. Reporting suspected privacy or security violations is part of everyone’s job. Do not fear any retaliation if you report a violation. Your organization cannot punish individuals who report violations. You should report violations or suspected violations to your facility’s privacy or information security officer. Your organization also may provide a way for you to report them anonymously, often through a compliance hotline.
In Conclusion

Protecting patients’ privacy is part of everyone’s job. It’s not enough for your hospital to have the right policies for protecting privacy. You must follow those policies and play an active role in your hospital’s compliance efforts. As you perform your job, remember the importance of patient privacy and security. This will help to ensure that your patients’ information remains private and that you remain in compliance with HIPAA.
1. You notice some papers with a patient’s name and other information in a trash receptacle. What should you do?
   
a. Ignore the papers because you don’t want to see confidential PHI. After all, you don’t need the papers for your job, and you don’t want to get into trouble.

b. Ignore the papers because they will be incinerated eventually.

c. Shred the papers or give them to your supervisor.

d. The papers cannot contain PHI because they are in the trash.

2. Which of these practices does not ensure security?
   
a. Tilting your computer monitor away from public areas

b. Locking laptop computers and other portable devices in secure containers or cabinets when not in use

c. Leaving a shared computer on so your coworker doesn’t have to log in again

d. Ensuring that doors and desks are locked appropriately

3. Which of the following items contains PHI?
   
a. An IV bag with a label containing a patient’s name

b. An advertisement for the hospital’s new cardiac center

c. A credit card receipt for balloons purchased in the gift shop

d. The names of the emergency room physicians
4. Under which circumstances may you disclose PHI that you access on the job?
   a. After you no longer work for the organization
   b. After a patient dies
   c. Only if you know the patient won’t mind
   d. When your job requires you to do so

5. You are helping to plan a surprise birthday party for your supervisor, but you aren’t certain whether her birthday is next Thursday or Friday. What should you do to confirm the date?
   a. You know she sees physicians at the hospital, so her birth date should be in her medical record. Ask a nurse or another staff member with access to the electronic medical system to check her record for you.
   b. Try to obtain a key to the storage room where her paper medical record is filed. You can check her file for her date of birth.
   c. Ask her supervisor. If the supervisor doesn’t know, flip a coin.
   d. Check her desk. She probably has paperwork from a recent physician visit that would include her date of birth.
6. Which of the following is the most secure password?
   a. T31Mottbg
   b. BBALLfan
   c. DavidOrtiz
   d. 2007WorldSeries

7. A new coworker, Elizabeth, just began working at your facility. However, she hasn’t yet received a user ID (login name), and she needs to look up some information on a computer. What should you do?
   a. Let Elizabeth borrow your login name and password just this once and then change your password afterward.
   b. Give her the login name and password of a former staff member who left last week. Chances are that the former staff member’s login name and password, which he kept under his mouse pad, will still work.
   c. Log on with your own login name and password and let her use your account for a few minutes.
   d. Speak with your supervisor. Then your supervisor can contact the technical support department to ask whether it can quickly get Elizabeth set up.
8. You’re at home at night, relaxing and wasting time on MySpace.com®. You check in on your friend, who is also a staff member at your facility, because she had a bad day at work. You see the blog that she has posted about her horrible day. Unfortunately, your coworker has described the unjust situations in full detail, and included patient names in her blog. What should you do?

   a. Send your coworker an e-mail and tell her that she might want to make the blog private because it contains PHI.
   b. Send your coworker an e-mail to tell her that she might consider deleting the blog completely to be safe.
   c. Speak to your privacy officer at work, because you think that many people may have seen your coworker’s blog that contained PHI.
   d. Nothing. Let your friend vent. You don’t need to betray your coworker and make her bad day even worse.

9. Whom should you call if you suspect that another staff member has violated HIPAA?

   a. Ghostbusters
   b. Your compliance officer or privacy officer
   c. The police
   d. Another staff member to obtain his or her opinion
10. You see someone familiar in the hall while you are headed to work. You quickly realize that, although you didn’t get a good look, you think it was your neighbor, Maria, being transported in a wheelchair. She didn’t tell you she’d be at your hospital. You want to find Maria to say hello and ask what happened. What should you do?

a. Ask around to attempt to learn what happened to her, whether she is a patient, and who treated her if she is.

b. Check the patient charts outside the rooms near where you saw Maria. You can probably find her room that way.

c. Call another neighbor to inquire about Maria. Maybe you’re the only neighbor who hasn’t heard about a recent accident.

d. Nothing. If Maria sees you and initiates contact, you can speak with her. Otherwise, you should not speak with her unless it is necessary to do so as a part of your job.
<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAMPLE
This is to certify that

___________________________________________________________________________________

has read and successfully passed the final exam of

HIPAA Handbook for Healthcare Staff:
Understanding the Privacy and Security Regulations

Lauren McLeod, Publisher