HIPAA Training Handbook for Telecommuters:

Privacy, security, and patients' rights

HIPAA *Training Handbook for Telecommuters: Privacy, security, and patients' rights* is published by HCPro, Inc.

ISBN 1-57839-433-3

HCPro, Inc., provides information resources for the healthcare industry.

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

Margret Amatayakul, RHIA, CHPS, FHIMSS, Author
Matthew Paul, Managing Editor
Lauren Rubenzahl, Copy Editor
Jackie Diehl Singer, Graphic Artist
Mike Mirabello, Senior Graphic Artist
Jean St. Pierre, Creative Director
Tom Philbrook, Cover Designer
Paul Nash, Group Publisher
Suzanne Perney, Publisher

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

Arrangements can be made for quantity discounts. For more information, contact:

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

Visit HCPro at its World Wide Web sites:
www.hcpro.com, www.hcmarketplace.com

05/2004
19539

Contents

About the author

Margret Amatayakul, RHIA, CHPS, FHIMSS

Margret Amatayakul, RHIA, CHPS, FHIMSS, is president of Margret\A Consulting, LLC, a health information management and systems consulting firm based in Schaumburg, IL. The firm focuses on providing synergies between healthcare regulations, such as HIPAA, and information technology, including electronic health records, point-of-care systems, and other clinical infrastructure issues.

Margret "A" has been instrumental in developing standards for privacy and security for highly regulated industries. She helped found and was the executive director of the Computer-based Patient Record Institute (CPRI), was formerly associate executive director of the American Health Information Management Association (AHIMA), and was on faculty at the University of Illinois at Chicago.

HIPAA Training Handbook for Telecommuters:

Privacy, security, and patients' rights

Intended audience

This handbook is intended for any members of a healthcare covered entity's work force or persons providing services to healthcare covered entities who have remote access to health information about patients. Such persons may include the following:

- Telecommuting staff who work for hospitals, physician offices, other types of healthcare providers, health plans, or healthcare clearinghouses (i.e., covered entities) and perform transcription, coding, billing, customer service, or other tasks for the entity for which patients' health information is accessed.

- Persons who work for companies providing transcription, coding, billing, help-desk services, remote information-technology and system-application support, radiology-film

review, and other services to healthcare covered entities where patients' health information is accessed.

- Healthcare professionals who provide services to patients in their homes, schools, places of employment, and other settings, such as home health nurses, school nurses, physical therapists working for sports teams, or mental-health counselors working for employee-assistance programs.

- Healthcare professionals who occasionally access protected health information from a virtual office or in a mobile situation, such as a physician who checks on the status of a patient from a computer in an airport lounge or via dial-up Internet connection from home.

This handbook acquaints those of you working in any of the above types of situations—collectively referred to as telecommuters—with the requirements for privacy and security under the Health Insurance Portability and Accountability Act of 1996, as well as the potential consequences of noncompliance. Its case scenarios illustrate the telecommuter's role in protecting patients' rights to confidentiality and securing the information from harm.

The basics

What is HIPAA?

Health information is the most personal data about an individual. When a person becomes a patient, the expectation is that his or her health information will be kept confidential and secure,

shared only with people who need the information to do their jobs, and kept safe from harm.

This expectation has always been a part of every healthcare professional's code of ethics. But as of April 14, 2003, when the Health Insurance Portability and Accountability Act of 1996 (HIPAA) took hold, this promise also extends to all who work with or may have access to health information. The law makes it illegal to violate a patient's privacy, which requires protection of individually identifiable health information, called protected health information (PHI).

HIPAA prescribes punishments for anyone who violates patient privacy. It also gives patients the right to gain access to their health records, request amendments to their health information, and limit the ways healthcare organizations use their information. It requires administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI. Many states already provide some or all of these protections and rights through existing statutes, but HIPAA federally mandates them for the first time.

HIPAA carries the potential for steep penalties. Those who intentionally compromise confidentiality for financial gain can be fined as much as $250,000 and sentenced to jail for up to 10 years. Even accidentally breaking the rules can result in fines—and tremendous embarrassment—for you or your employer.

What does this law address?

HIPAA is a broad law that covers a variety of issues. One of its

goal is to enable people to easily move from one health insurance plan to another when they change jobs or become unemployed. This is the "health insurance portability" component. Another goal is to create penalties for those who defraud healthcare-benefit programs. This goal is addressed in the fraud and abuse provisions that represent the "accountability" component.

In addition to addressing portability and accountability, administrative simplification provisions provide standards for privacy and security. Privacy refers to an individual's right to maintain control over his or her personal information. HIPAA provides rules for covered entities about when confidential health information may be used and disclosed, what rights patients have with regard to health information maintained by healthcare organizations, and what measures healthcare organizations must take to protect the information. Security refers to technical controls over information in electronic form. These controls help keep personal information confidential and free from alteration, destruction, or loss. HIPAA provisions also require all healthcare providers and payers to use standard formats for common financial and administrative transactions (i.e., submitting claims on a patient's behalf), and to use national standard identifiers for providers, health plans, and employers. Standard identifiers require each provider, health plan, and employer to use a unique national identifying number rather than have every entity create one for itself and for providers and employers.

Because so many people are involved in providing healthcare-related services and so much health information is being stored

and transmitted electronically, the HIPAA privacy and security rules were created to assure the public of protections for and rights to their health information.

What are the consequences for noncompliance?

Breaking HIPAA's privacy and security rules can lead to civil and criminal penalties.

Civil penalties include fines of up to $100 for each violation of a requirement of the law per person, with a limit of $25,000 for each requirement. For example, if a hospital illegally released 250 patient records to a marketing company, it could be fined $100 for each wrongful disclosure, for a total of $25,000. If the hospital also could not account for the disclosures to the marketing company when 250 patients asked the hospital for an accounting of disclosures, the hospital could be fined another $25,000 for violating the requirement that it must supply a list of disclosures of PHI it has made for other than treatment, payment, and operations purposes upon request of the patient. If an insurance company did not implement access controls so that only authorized staff had access to patients' health-insurance information, the company could be fined $100 for each time an unauthorized staff member gained access to such information.

Criminal penalties include large fines as well as jail time. The penalties increase proportionately with the seriousness of the offense. For example, selling patient information for personal gain

is more serious than an accidental release, so it brings stiffer penalties. These penalties can include fines as high as $250,000 and a prison sentence of up to 10 years. The following are examples of violations and possible penalties:

- Knowingly releasing patient information in violation of HIPAA can result in a one-year jail sentence and $50,000 fine
- Gaining access to health information under false pretenses can result in a five-year jail sentence and a $100,000 fine
- Releasing patient information with harmful intent or selling the information can lead to a 10-year jail sentence and a $250,000 fine

What is PHI?

PHI is information that identifies a patient and describes his or her healthcare status, illnesses, injuries, and treatment. HIPAA specifies numerous identifiers that relate to a patient, the patient's relatives, employers, or household members. The most common examples of these identifiers include

- name
- address
- telephone number
- fax number
- e-mail address
- birth date
- admission date

- discharge date
- date of death
- all ages over 89
- Social Security number
- medical record number
- health-plan beneficiary number
- account numbers
- full-face photographic images
- any other unique identifying number, characteristic, or code

HIPAA defines health information as any information created or received by a healthcare provider, health plan, or other entity that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. Typically, such information includes the following:

- Diagnoses, problems, complaints, injuries
- Health history and physical exam findings
- Current and past medications
- Observations of health status, vital signs, response to therapeutic procedures
- Laboratory tests and other diagnostic studies and their results
- Surgical procedures and other treatments
- Summaries of healthcare services and healthcare correspondence
- Healthcare claims, description of proposed healthcare services for eligibility determination or referral authorization

If any identifiers are associated with any health information about the person, the information is protected by HIPAA, and thus called PHI.

Who is authorized to see PHI?

Many people have access to PHI for a variety of reasons. Physicians, nurses, pharmacists, therapists, dietitians, healthcare technicians, and others use this information to determine how to treat patients. Transcriptionists listen to such information in order to convert dictation into typed form. Coders and billers use PHI to bill patients, their insurance companies, Medicare, or Medicaid for services. Persons performing quality-assurance and performance-improvement activities may review PHI to make sure patients are receiving high-quality services. Customer-service representatives in a health plan or health-insurance company may need PHI to determine eligibility for benefits, provide authorization for reimbursement of services, or adjudicate claims.

Sometimes access to PHI is only incidental to the task being performed. Still, it is important to recognize your obligation to keep such information confidential and secure. For example, you may be an information-systems technician providing help-desk services, such as troubleshooting computer problems for users. Because it may be necessary to view a screen containing PHI in order to solve a computer problem, your access to the information is an incidental disclosure. Likewise, you may be repairing a medical device that contains information about the past several diagnostic tests for patients or the past several hours of vital signs

for a patient. You must make sure this information remains confidential and that no wrongful disclosures are permitted.

HIPAA makes distinctions between covered entities and business associates. A covered entity is a healthcare provider (e.g., hospital, nursing home, ambulance service, physician office, etc.), health plan (e.g., health insurance company, Medicare, Medicaid, or other type of organization that pays the cost of healthcare—also known as a payer), or healthcare clearinghouse (i.e., company or service used to translate and transmit healthcare claims). Every covered entity must ensure that members of its work force comply with HIPAA. A covered entity's work force includes not only employees, but any volunteers, trainees, and others who work under the direction of the organization, whether or not they are paid by the organization.

A business associate is a person or company that provides services for a covered entity and uses or discloses PHI in the process. Business associates may include transcription companies, medical-billing services, outsourced coding consultants, health-information systems vendors, utilization-review companies, accountants, management service companies, and many others. A business associate must have a contract with the covered entity in which it agrees that its work force will protect any information to which it may have access in the performance of its services.

Not every company that provides services is necessarily a business associate. For example, the telephone company representa-

tive who installs cable service to your home so you can provide telecommuting services would never have access to PHI for any function being performed and is not a business associate. The express mail courier who delivers typed reports to a physician's office from a transcriptionist would not have access to the PHI contained within the sealed envelope and therefore is not a business associate. Unless a company in the normal course of business must have access to PHI, the company is not a business associate.

How much can you see?

All members of the work force at a covered entity and business associates contribute to the quality of healthcare or payment services in some way. But that doesn't mean everyone needs to see patients' health information about patients. Many employees have no access to patient information—on computer or on paper—because they don't need it to perform their jobs. For example, a hospital orderly should not have a password to gain access to electronic medical records. Custodial-services staff at a health plan do not need PHI to perform their jobs, so paper containing PHI should be shredded or locked up while awaiting destruction.

HIPAA requires members of the healthcare work force to use or share only the "minimum necessary" information they need to effectively do their jobs. For example, coders need to look at the entire record of a patient's hospital stay to apply all the correct codes. However, perusing the correspondence section of the record is unnecessary and inappropriate.

The minimum necessary requirement does not apply when a healthcare professional has a treatment relationship with the patient. In such a case, the healthcare professional should have access to all health information about the patient in order to provide the best healthcare services possible. Healthcare professionals can look at their patients' entire records and freely share information with other healthcare professionals who care for those patients.

However, if a healthcare professional is not treating the patient or conducting other functions authorized by the covered entity (i.e., quality review) or the patient (i.e., research), then he or she may not access the PHI. Minimum necessary also does not apply when the patient has explicitly authorized disclosure. This means that patients can authorize disclosure of their entire medical record to anyone they wish. Before looking at any patient information, ask yourself: Do I need to know this to do my job? What is the least amount of information I need to do my job?

Depending on your job, you may have considerable or very limited access to PHI. For example, if you are a medical coder working from home and have been assigned specific cases to code, you may be sent copies of only those medical records and no others. It is your duty to ensure that these copies remain safe in your home, that family members and others who visit do not see the records, and that you either properly destroy the records or return them to the provider as specified in your service contract.

As a telecommuting coder, you may be given access to an information system that has scanned the medical records. You may only access those records assigned and make copies of allowed items. You also must ensure that no one can read the records over your shoulder when you are working on them or see them on the screen when you leave your work area.

Similarly, if you are a home health nurse, you may share detailed information about a patient with his or her physician and other healthcare providers, such as nutritionists. You may share limited information with an individual designated by the patient as a caregiver. However, be careful not to leave any information in view of neighbors who may come to visit. Even if you know the neighbors are concerned about the patient, do not reveal any PHI you've learned in the course of your job unless the patient has indicated he or she wants the neighbor to have limited information in the event of a problem.

These rules apply even when you no longer work for the healthcare organization or business associate. Just because you know a hospital treated a certain celebrity does not mean you can reveal PHI about the person after you leave the employment of the hospital or the business associate providing services to the hospital.

Who oversees privacy and security policies?

HIPAA requires each covered entity to appoint a privacy official and an information security official. These persons are responsible for developing and

implementing an organization's privacy and security policies. Many business associates of healthcare covered entities have also created such privacy and security positions.

If you telecommute for an organization that has an information privacy official and an information security official, get to know them. They can provide considerable assistance to ensure you are meeting HIPAA's privacy and security rules. If you are self employed, you automatically become your own privacy and security official. Establish your own policies and procedures as evidence that you are doing the right thing. You probably have already been approached by the healthcare covered entities for which you work to sign a business associate contract.

The following are key rules to follow in protecting health information, whether you work for a covered entity, work for a business associate, or are a business associate yourself:

- Do not leave your computer logged on to any patient-information system while you are not at the computer. Do not leave copies of paper medical records unattended.

- Position your computer so no one can view the screen while you are working on it. If you work from home, ensure that you have a work area that does not have frequent traffic, such as the dining room table or kitchen counter. If you are mobile while telecommuting or use a personal digital assistant, tablet PC, notebook computer, or other such device, make sure you always have it with you or lock it out of view (such as in the

trunk of a car rather than leaving it in the back seat). If you are a healthcare professional, you may already take precautions to ensure that you do not display any indications of your business for safety reasons. Apply the same precautions to your computer.

- Carry out discussions about patient care or the PHI you use in a private area and in a low voice to the extent possible to reduce the likelihood that visitors and others will overhear you.

- Keep good records of how you handle PHI. If your computer connects to an information system at the covered entity or business associate, it should provide means to authenticate you (i.e., using a password, keycard, or other device). The information system should also provide controls on what you may access and keep an audit trail of what you have seen or worked on. If you do not directly connect to a computer system, but instead use paper copies of PHI, make sure that when they are no longer needed they are always shredded or placed in locked receptacles for delivery to a recycling company that will destroy them. They must never be left whole with the garbage.

- If you connect electronically to a covered entity or business associate, make sure you have a separate phone line or other dedicated connection for the transmission. Follow any instructions from the covered entity or business associate about logging in, using encryption, maintaining anti-virus

software, having a power-surge protector, and other security requirements. Do not attempt to bypass any of these measures—they are as much to protect you from being accused of wrongdoing as they are to protect the information itself.

These suggestions are all basic ways to protect the confidentiality of PHI, ensure PHI is not incorrectly altered, and maintain accessibility to PHI when needed. For example, the power-surge protector does not provide confidentiality, but it does ensure that data are not lost or corrupted when you are using your computer and there is a power outage.

Many covered entities are doing more to protect PHI when employing telecommuters. For example, if paper medical records are scanned into a computer system to which remote coders have access, identifying information can be masked or encoded. Some organizations ask persons who dictate to identify the patient using a code to reduce the chance that the patient's identity will be revealed.

However, some telecommuting tasks require positive identification of a patient, in which case such deidentification measures are not appropriate. For example, a physician may be contacted at a restaurant about a patient. This example may not seem like telecommuting, but in essence it is. The physician needs to know who the patient is, but just the same should take precautions not to reveal the patient's identity to others. For example, it may be appropriate to find a private place to speak on the phone. It may

even be necessary to find a land line rather than a mobile phone to conduct certain conversations.

The most important measure in truly providing privacy and security is the human element. You must not share information you hear or see in the course of your work. Take appropriate precautions to ensure that others do not hear or see PHI. Comply with the rules to protect patients' confidentiality to ensure their data are not inappropriately altered and that they are available when needed. Not taking these precautions is a violation of the law.

What if I know someone has broken the rules?

During the course of your work, you may find that someone is not adhering to privacy and security policies. Anyone who notices such behavior is encouraged to report violations or suspected abuses to the organization's privacy or security officials. Do not fear any retaliation if you report a violation. Under the law, the organization cannot punish you for reporting violations. In fact, it is part of your job to report instances where you suspect that privacy or security policies are being broken.

Case #1

Your sister's close friend is having surgery at the hospital where you telecommute. She asks you to find out what you can about the friend's condition. Should you call and ask the nurses you know? Should you look up the friend's medical record?

The answer is no. Even if you and your sister have the best intentions, you have no right to look at private information about her friend's health.

Looking at patient records for any nonbusiness reason is cause for dismissal and can have possible legal consequences. If you share or repeat confidential information that you discover, either deliberately or by accident, you can lose your job.

This rule applies to all employees, whether working on the premises or from home. Protecting confidential information is a responsibility that the entire work force shares, regardless of where its members work.

Case #2

A woman tells you she is at the hospital to work on the computers and wants you to give her your password to troubleshoot your computer. How do you respond?

Under no circumstances should you give anyone your password. Even if you recognize the person's voice and know the person well, computers can always be fixed without a password. At most, a computer technician may tell you that your password will be disarmed to conduct repairs and that you will need to enter a new and different password later. The best response to a person asking for a password is to indicate you cannot give out that information, disconnect, and report the incident to your supervisor or information-security official.

Case #3

As you are transcribing an operative report, you realize a patient is an acquaintance of yours. Should you call him to find out how he's feeling?

No. If you learned of your friend's condition only because you happened to see his name on a record, you should not call him, nor should you mention what you found out to anyone else. Your friend may not want anyone to know about the surgery, and it is his right to keep it private. If this patient wants you to know he is recovering from surgery, he will tell you or ask a friend or family member to contact you.

Case #4

You place paper containing PHI in a locked bin that a shredder service picks up each week. It is nearly overflowing and you have a list of patients' last names and medical-record numbers that you were checking to ensure that you had billed for all patients that week. Can you toss the list in your household garbage can instead?

No. Any paper that includes identifying patient information must be securely disposed of. If you are at home, it may be possible to incinerate or burn the paper, although it is probably better to get a larger bin or your own shredder.

Computer systems and electronic information transmission

What security measures are needed?

There are many benefits of telecommuting for the healthcare organization and the individual telecommuter. But there are also unique issues and heightened risks. Outsourcing—especially involving workers outside of the United States—has become controversial. As a telecommuter, you can minimize risks for your customers if you address them head on.

HIPAA does not specify what form of agreement should be in place for telecommuters. In fact, HIPAA does not treat telecommuters differently than any other members of the work force of a covered entity or business associate. However, the healthcare covered entity or business associate using telecommuters likely will want to have an agreement with the telecommuter concerning the telecommuting arrangement, including ownership of the computing equipment and all other matters relating to the telecommuting process, including many non-HIPAA issues (e.g., hours expected to be working, insurance coverage, ergonomics to keep Occupational Safety and Health Administration injuries in check, use of subcontractors, and—for international telecommuters—specification of international law that pertains to the contractual arrangement).

The agreement may vary based on whether you are telecommuting as an employee of a healthcare covered entity or business associate, or if you are a business associate yourself. As a

telecommuting employee, look upon such an agreement as a means to protect your interests and the interests of your employer. If you are in business for yourself, telecommuting may be covered in a larger agreement that also includes business associate requirements.

If you are only an occasional remote user, a formal telecommuting agreement may sound like overkill. However, remote computing of any kind is a serious matter that merits careful consideration.

Certification

One important issue to address is ownership of computing equipment, which includes not only the computer itself, but all peripheral devices such as printers, external storage devices, and network devices.

If the organization owns the devices, it should be spelled out clearly in the telecommuting agreement. Organizations are generally advised that the agreement should limit the use of the devices to the organization's business. The telecommuter should not use the devices for any other purpose, load any personal software on them, or attempt to repair anything without permission. The nature of the security mechanisms applied should be understood, and the telecommuter should not make any alterations. Again, these precautions are as much for your protection from liability as the organization's protection for privacy and security.

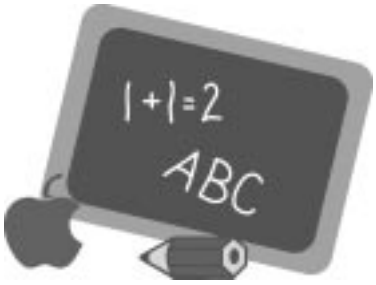
If you use your own equipment, an agreement may require certification of the equipment to ensure that appropriate security is in

place. The agreement should specify certification requirements, who will perform the certification, who pays for the certification if it is required to be performed by a third party, and how frequently the certification must be renewed.

Contingency planning

HIPAA's security rule requires contingency planning—having both routine backups and emergency-mode operation and disaster-recovery plans. The telecommuting agreement should specify what backups you may or must make, under what circumstances they are made, for how long you must keep them, and how they must be destroyed or returned. Contingency planning also should consider how data/computing equipment at your telecommuting location will be retrieved in the event of prolonged illness or termination.

Training



Ensure that you are properly trained on both privacy and security matters. If you work for a covered entity or business associate, you may be included in the organization's privacy and security training program. If not, consider how you will keep yourself informed and up to date on privacy and security matters. There are many excellent free materials available from various Web sites, and many professional associations have

local and regional chapters that provide low-cost seminars. Investing the time and resources to be trained—and maintaining documentary evidenced of the training—can be an important factor in protecting yourself.

Policies

Policies are another important element in ensuring privacy and security, and how they are addressed in the telecommuting environment likely will vary depending on whether you are an employee or business associate, or are self employed. If you are working for a covered entity or business associate, you will be expected to adhere to your employer's policies. If you are self employed, it is a good idea to have some of your own policies. At a minimum, your policies should outline the measures you take to protect privacy and implement security. They should define what breaches of confidentiality and security incidents are, and to whom such events should be reported. Again, documentary evidence of planning for privacy and security is an important measure of the professionalism of your business.

Physical controls

It has already been mentioned that your workstation should be properly positioned to avoid incidental disclosures, that you should dispose of anything containing PHI in a secure manner, and that you should perform any applicable backups. Physical facility controls may also be included in a telecommuter agreement. These might require you to have a smoke detector, fire extinguisher, locking file cabinet, power-surge protector, and

other reasonable physical safeguards. The agreement might also require a workplace inspection.

It is always a good idea to have a physical inventory of the equipment and furniture in your workplace. You may want to place a copy of an equipment inventory, with serial numbers, in a safe deposit box. Even if you do not own the equipment, it is a good idea to have verification of what has been placed in your environment.

Technical controls

User IDs, passwords, and other forms of authentication security features help prevent unauthorized access to the computer system and protect patient information.

If you have password access to an organization's computer system, never give your password to anyone or log in to the health information system using someone else's password—even if it seems like a timesaver. HIPAA requires organizations to be able to tell who looks at what records so they can make sure all uses of PHI are necessary and appropriate. Your organization will most likely do that by keeping track of the user names and passwords used to gain access to the system.

Avoid passwords that can be easily guessed, such as your child's or pet's name, your birth date, and any word that could be found in the dictionary. Use a combination of letters and numbers and uppercase and lowercase. Doing so makes your password more

difficult to crack. If you have a hard time remembering your password, try using the first letters of song line, or book, TV program, or movie title in unique ways. For example, 0S3UC? may represent "Oh Say Can You See?" where a zero is used in place of the O in Oh, S is the first letter in Say, a 3—as the third letter in the alphabet—is used to represent the C in Can, U is the pronunciation of You, and C the pronunciation of See. With letters, numbers, and special characters, this six-digit password meets all the requirements of a strong password and is easy to remember because you created it with something you know well.

In addition to creating strong passwords, understand what form of transmission you are using to send and receive PHI, and what security features the transmission media include. For example, if the covered entity sets you up with a virtual private network (VPN), this enables very secure transmission of PHI from your telecommuting site to the covered entity. However, if you use a dial-up connection to transmit reports via commercial e-mail services over the Internet, this is not secure at all. The business associate contract you have with a covered entity should identify for you the nature of transmission security controls it expects you to use. If it is necessary to establish a digital signature or use encryption, be sure you always apply these measures.

Faxes

Faxes have become widely used and tend to be more prone to error than other forms of communication. Faxed patient information can easily fall into the wrong hands, which would be a vio-

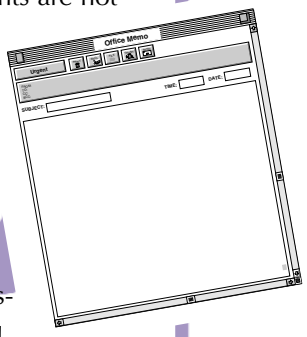
lation of the privacy rule. Before faxing any patient information, check the applicable policy to make sure you follow faxing guidelines.

When you fax patient information, you should ideally send information to a dedicated fax machine in a secure location and notify the intended recipient when you are about to send it so he or she can be ready to pick it up.

If you know you will receive a fax that contains patient information, tell the person faxing the information to warn you ahead of time so you can be present to receive it. Consider using an electronic fax service so faxes do not accumulate on a machine that is available to others in your home, at a hotel registration desk, or at another remote location.

E-mail

Like faxes, e-mails have become widely used and are prone to error. Check the applicable organization's policies about the use of e-mail. If you have access to your employer's e-mail system, remember that employer e-mail accounts are not meant for personal use. Sharing or opening attached files from unknown sources can open the door to viruses and hackers.



Keep in mind that you can never be sure who will have access to your message on the receiving end. Never send

confidential information about a patient in an e-mail over a public network unless the organization's policies allow it. If they do, make sure the use of e-mail meets the criteria in the policy and follow the procedures established to protect the message from being intercepted or altered during transmission.

When you send e-mail, always double check the address line just before sending the message to be sure your message doesn't go to the wrong person or list by mistake.

Case #5

A physician calls you to request that you fax a patient's report to her office. However, her office is closed and no one will be able to pick up the fax until morning. What should you do?

Don't send the fax to an unattended machine unless the doctor assures you that the machine is in a locked room, has a locked cover, or places faxes in memory to be printed upon execution of a physical command.

If the fax machine is out in the open, arrange to fax the report to the office during regular business hours when a staff member at the office can wait for the fax and pick it up immediately.

Case #6

A fellow telecommuting transcriptionist is having trouble logging in to the facility's system. He asks for your login name and

password so he can try them. Should you share them with him?

No. HIPAA requires the use of unique passwords for each user who has been authorized access to PHI stored in the computer system. The facility keeps track of the records you look at based on the user ID and password you use to enter the system. If you let others use your ID and password, you are breaking HIPAA's rules and may be held responsible if your coworker gains access to patient information inappropriately.

It is a good idea to change your password regularly—especially if you know someone has gained access to it.

Case #7

Because you have to change your password for the computerized record system every 90 days, you have a hard time remembering it. Should you jot it down on a piece of paper and stick it in your desk drawer?

No. Even if your drawer remains locked, every time you open it there will be an opportunity for others to see your password. Do not write down your password because someone who is intent on finding it will know all the (not-so) secret places one could possibly think of to attempt to keep a password safe. Once someone has learned your password, it takes no time at all for him or her to gain access to

PHI. He or she could introduce viruses and other malicious software into a system and cause the computers harm.

Case #8

Your daughter needs to use the Internet to do research for a history project, but your family computer is broken and you don't have time to take her to the library. All of your work-related files are password-protected. Should you let your daughter use your work computer?

No. If there is confidential patient information on your computer, you cannot let others use it. The only way to be absolutely certain that others won't come across the confidential information on your computer is to prevent them from using the computer altogether.

Case #9

You're waiting to be seated at a busy restaurant and want to check to see whether a physician has responded to your query about a patient's diagnosis. You have your PDA with you and can log in to the hospital's computer system to see whether the physician has responded. What should you do?

If your facility's policies allow it, you may log in to the system and find out the information you need, but not in the middle of a busy restaurant. Move to

a private location, such as your car or an empty room, where no one else but you will be able to view the information.

Patient privacy rights

As a telecommuter, you may not have the same responsibility for addressing patients' privacy rights as those who work directly in a healthcare covered entity. But it is still important for you to be aware of these rights. If you are a business associate, you may be required under certain limited circumstances to make certain PHI available to patients, make PHI in your possession available for amendment, and provide an accounting of disclosures.

Notice of privacy practices

HIPAA requires covered entities to have a notice explaining the different ways they may use and disclose patient information so patients understand how providers and health plans protect their information. This document, called the notice of privacy practices, also tells patients or members of health plans that they have the following rights:

- Right to receive a notice of privacy practices when they begin receiving care from an organization or benefits from a health plan, and any time there is a material change in the notice (and at least every three years from their health plan). This notice explains to individuals how their PHI will be used and disclosed, what rights they have in their PHI, and what administrative measures are taken to protect their PHI.

- Right to access their health information. This right includes the ability to see and obtain copies of one's own PHI, unless a healthcare professional believes the person could be harmed by having the information or if there is some legal reason to withhold access. The individual has the right to appeal a denial for access.

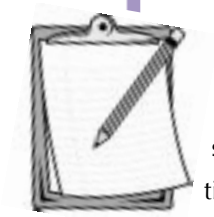
- Right to request amendments to their health information. If an amendment is accepted, it cannot eradicate an original entry, but should be linked to the original entry and disclosed to others who may have relied upon the original information. A covered entity does not have to accept an amendment offered by an individual if the entity believes the original information is correct or if the information was not created by the entity. As with an individual's rights with respect to access, the individual also has the right to file a statement disagreeing with a denial of amendment, and this statement must accompany the information any time it is disclosed to others.

- Right to request restrictions on uses and disclosures of their health information. For example, a patient may ask that a certain person who works in the health information management department not have access to the person's PHI. The hospital may reject the request if it is not able to ensure that the restriction can be managed.

- Right to obtain an accounting of disclosures. This is a list of when the covered entity has provided someone outside of its

organization PHI about the individual, except when the disclosure was for treatment, payment, and healthcare operations, or in instances in which the patient authorized a disclosure. For example, when a hospital reports a person's communicable disease to the state's public health department, it must account for this disclosure if the person asks for an accounting. However, if the patient is being referred to another physician for treatment and the hospital provides the physician a summary of the patient's care, this disclosure is for treatment purposes and does not get listed on the accounting.

Authorization



As a telecommuter, you may be in a position to release information from a covered entity. If you routinely perform such operations, you should be intimately familiar with the organization's policies about when an authorization signed by the individual is required. If you generally do not release information, a quick overview of the authorization requirements under HIPAA should be sufficient to alert you to when you need to refer an individual to have the proper procedures performed.

In general, when a covered entity needs to use or disclose patient information for purposes other than treatment, payment, or routine healthcare operations, it must obtain an authorization from the patient. For example, it must seek authorization to sell mail-

ing lists to marketing companies or to use information for research purposes. By way of the authorization—which must be in writing—patients voluntarily agree to let the organization use their information only for a particular purpose.

Patients are permitted to revoke authorizations at any time. After an authorization has been revoked, the facility no longer is allowed to use or disclose the information for the purpose documented in the authorization. However, uses or disclosures made before the patient revoked the authorization are not affected.

HIPAA prohibits facilities from requiring patients to sign authorizations. They must provide care regardless of whether the patient agrees to allow disclosure of his or her health information beyond the scope of treatment, payment, and routine operations.

It should be noted that if state law is more stringent (i.e., affords greater protection of privacy), then state law prevails. It is quite common for state law to be more restrictive in the area of authorizations. For example, some states require an authorization for disclosure of health information to another provider for treatment purposes. Depending on where a disclosing organization is located, it may have stricter state laws with which to comply.

Psychotherapy notes

Psychotherapy notes have much stronger protections than other PHI because these are personal notes of the treating psychotherapist that can be damaging not only to the patient but potential-

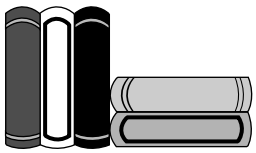
ly others if they fall into the wrong hands. Under HIPAA, providers must obtain separate authorizations to disclose psychotherapy notes for any purpose—even treatment, payment, and routine operations.

However, the privacy rule narrowly defines psychotherapy notes. These are not normal records of mental health, behavioral health, or substance abuse. Psychotherapy notes are defined as follows:

> *"Notes recorded (in any medium) by a healthcare 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 separate from the rest of the individual's medical record.*
>
> *"Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."*

Patients' right to inspect and copy their PHI does not extend to psychotherapy notes.

Laws requiring disclosure without authorization



There are several circumstances in which PHI may be disclosed without authorization, such as for law enforcement, public health, abuse reporting, and healthcare oversight purposes; when there is a court order; to coroners, funeral directors, and for organ donor purposes; for preresearch in certain limited circumstances; to avert a serious threat to health or safety; and for specialized government functions. These disclosures are described briefly in the notice of privacy practices.

If you are asked to carry out any such disclosures, be sure you understand the organization's policies before releasing information. Never give out PHI without confirming that the person or agency requesting the information has a legal right to it.

Right to complain

HIPAA calls for organizations to designate a contact person or office for receiving complaints of privacy violations. The name of a contact person or office must be included in the organization's notice of privacy practices.

HIPAA also requires covered entities to identify that persons have the right to file a complaint with the federal government.

Complaints concerning privacy issues are to be directed to the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), which is charged with enforcing the privacy

rule. The Centers for Medicare & Medicaid Services (CMS) is responsible for enforcing the security rule and transactions and code sets rule.

Deidentifying information

Medical researchers often need information in medical records to do their jobs effectively. But it can be impractical to seek authorization from all the patients whose records are sought for a research study.

That's why HIPAA allows researchers to use deidentified PHI from records without individual authorization. In these cases, facilities remove all identifiable information before allowing researchers to use it.

Providers can give researchers a limited data set, which includes indirect identifiers such as certain birth dates, city information, and ZIP-code information. Recipients of a limited data set must sign a data-use agreement, which restricts their use of the information to a specific purpose.

Patient directories

Facilities can list certain information about each patient in their patient directories. However, organizations must give patients the opportunity to opt out of inclusion in the directory or to restrict the amount of information available in the directory. If a patient agrees to be listed in the directory, the following information can be given to visitors or callers who ask for the patient by name:

- Location in the facility
- General condition (e.g., stable, good, fair, etc.)

If a patient opts out of the directory entirely, staff should not provide any information to callers or visitors, including whether the patient is at the facility.

Directories may also include religious affiliation, but this information is reserved exclusively for clergy. Facilities may give the names, locations, general conditions, and religious affiliations of all patients in the directory to clergy who request the information. Members of the clergy are not required to request the information by name. Facilities may not provide information for patients who have opted out of inclusion in the directory.

HIPAA does not require facilities to keep directories or ask patients their religious affiliation. But if the facility does have a directory, it must follow HIPAA's rules for allowing patients to opt out and respecting those requests.

Case #10

A scientist from a local nonprofit organization is researching cancer treatment and wants to see the records of all patients treated for breast cancer in the past year at the hospital for which you work as a remote coder. Can the records be released to him?

No. In order to allow the scientist to view the records, your facility must either obtain authorizations from every patient whose record you plan to release or it must remove the identifying information so the researcher has no way of knowing who the patients are. The researcher could also obtain a waiver from a federally regulated institutional review board or privacy board allowing the disclosure of the records without deidentification when it has been deemed there is minimal privacy risk.

Case #11

A patient knows you are a business-associate transcriptionist for her physician, and she has requested that the physician not send any dictation to you. Should the physician comply with this request?

Yes. Although the physician has the right to refuse a request for restriction in cases where she could not reasonably comply with the request, this request would probably be relatively easy to comply with. The physician could use a different transcription service, handwrite, or type the material normally dictated.

Case #12

A patient comes to the emergency room and requests that no one be told he is in the facility. A woman comes to the emergency room and asks for the patient by name, identifies

herself as the patient's mother, and shows her driver's license in an effort to prove her relationship. What should the woman be told?

Unless healthcare professionals believe in their professional judgment that the disclosure is in the best interest of the patient, the facility is not permitted to tell the woman anything, including whether he is even at the facility. If a patient requests his name not be included in the facility directory, facility staff are not permitted to give out any information about him to anyone, regardless of the individual's relationship to the patient.

To avoid a customer-relations problem, it may be appropriate to provide a copy of the notice of privacy practices to the mother, explain that patient privacy is of the utmost importance, and indicate that if any patient requests confidentiality, the facility abides by that request.

Final exam

True or False?

1. The criminal penalties for improperly disclosing PHI can include fines of up to $250,000 and prison sentences of up to 10 years.

2. Privacy protections cover patients' health-related information, such as the reason for treatment, when the information is identifiable by patient address, age, Social Security number, or phone number.

3. Passwords should be a minimum of six characters and should include both letters and numbers or other special characters.

4. You must retype a report when the patient has requested an amendment to the document.

5. Facilities must obtain authorization from new mothers before sending their names and addresses to a local cloth diaper service who will send the mothers coupons and literature about their services.

6. Coders who work from home are advised to use their family computers to do their work rather than a computer provided by their employer.

7. A case manager working for a health plan may log on to a computer from a hotel to review her case load.

8. Remote transcriptionists should have a contingency plan that spells out what they would do if their computing equipment is damaged.

9. A customer-service representative may not have access to any PHI.

10. A physician completing records at home in the evening would probably be best served by using a notebook computer in the family room.

Multiple choice

11. A man comes to your home office and tells you he is supposed to set up the hospital's computer you use with special new anti-virus software. How should you respond to this request?

a. Provide him with the access he needs
b. Ask him who at the organization hired him and verify with that person
c. Call the police
d. None of the above

12. Your sister's friend just had triple bypass surgery at one of the facilities for whom you provide coding services. She asks you to find out his prognosis. What should you do?

a. Call a nurse you know on the floor and pass the information along to your sister
b. Log in to the computerized record system and read the patient's record to find information for your sister
c. Explain that it's a violation of the patient's privacy for you to ask around or look at his record, and suggest that she call one of her friend's family members
d. None of the above

13. Under what circumstances are you free to repeat to others' PHI that you hear on the job?

a. After you no longer work at the organization
b. After a patient dies
c. Only if you know the patient won't mind
d. When your job requires it

14. Which of the following are common features designed to protect confidentiality of health information that you may keep in your home office?

a. Lock on the door of the home office room
b. Password to gain access to computerized records
c. Rule that prohibits anyone other than an authorized representative of the hospital from looking at records
d. All of the above

15. You notice that several files on the computer you use as part of a billing service for physician offices are corrupted. What should you do?

a. Ignore the problem; it was probably something you mistakenly did
b. Fix the problem by running your anti-virus software
c. File an information-security incident report with the physician office
d. None of the above

16. Which of the following does HIPAA require if you are a business associate?

a. A business associate contract
b. An agreement that your workplace follows OSHA requirements for injury prevention
c. A home inspection
d. All of the above

17. When is the patient's authorization to release information required?

a. In most cases in which patient information is going to be shared with anyone for reasons other than treatment, payment, or healthcare operations
b. Upon admission to a hospital
c. When patient information is to be shared among two or more clinicians
d. When patient information is used for billing a private insurer

18. You have been asked by a physician to start sending claims you code for her directly to the health plan. What should you do?

a. Deny the request because it is against HIPAA regulations
b. Send the claims to the health plan through your commercial e-mail system
c. Establish an agreement with the health plan regarding how you will send the claims
d. Hire a healthcare clearinghouse to send the claims for you

19. Which of the following is an incidental disclosure?

a. A patient sign-in sheet at the dentist office
b. A patient's medic-alert bracelet
c. A conversation with a patient who is hearing impaired that is overheard from another examining room
d. All of the above

20. Which of the following types of information does HIPAA's security rule protect?

a. Patient information in electronic form
b. Patient information communicated orally
c. Patient information in paper form
d. All of the above

_____

(Sign your name on the above line if you have completed this quiz.)

Answers to the final exam

1. T
2. T
3. T
4. F
5. T
6. F
7. T
8. T
9. F
10. F
11. b
12. c
13. d
14. d
15. c
16. a
17. a
18. c
19. d
20. a

Need more copies? That's easy

Call customer service at 800/650-6787 for more information or to order additional copies. For bulk ordering information, see below.

Call: 800/650-6787

E-mail: *customerservice@hcpro.com*

Internet: *www.hcmarketplace.com*

Mail to: HCPro, Inc., P.O. Box 1168, Marblehead, MA 01945

Fax: 800/639-8511

For special pricing on bulk orders, please call Dave Miller toll-free at 888/209-6554.

Certificate of Completion

This is to certify that

_____

has read and successfully passed the final exam of

HIPAA Training Handbook for Telecommuters: Privacy, security, and patients' rights

Suzanne Perney

Vice President/Publisher