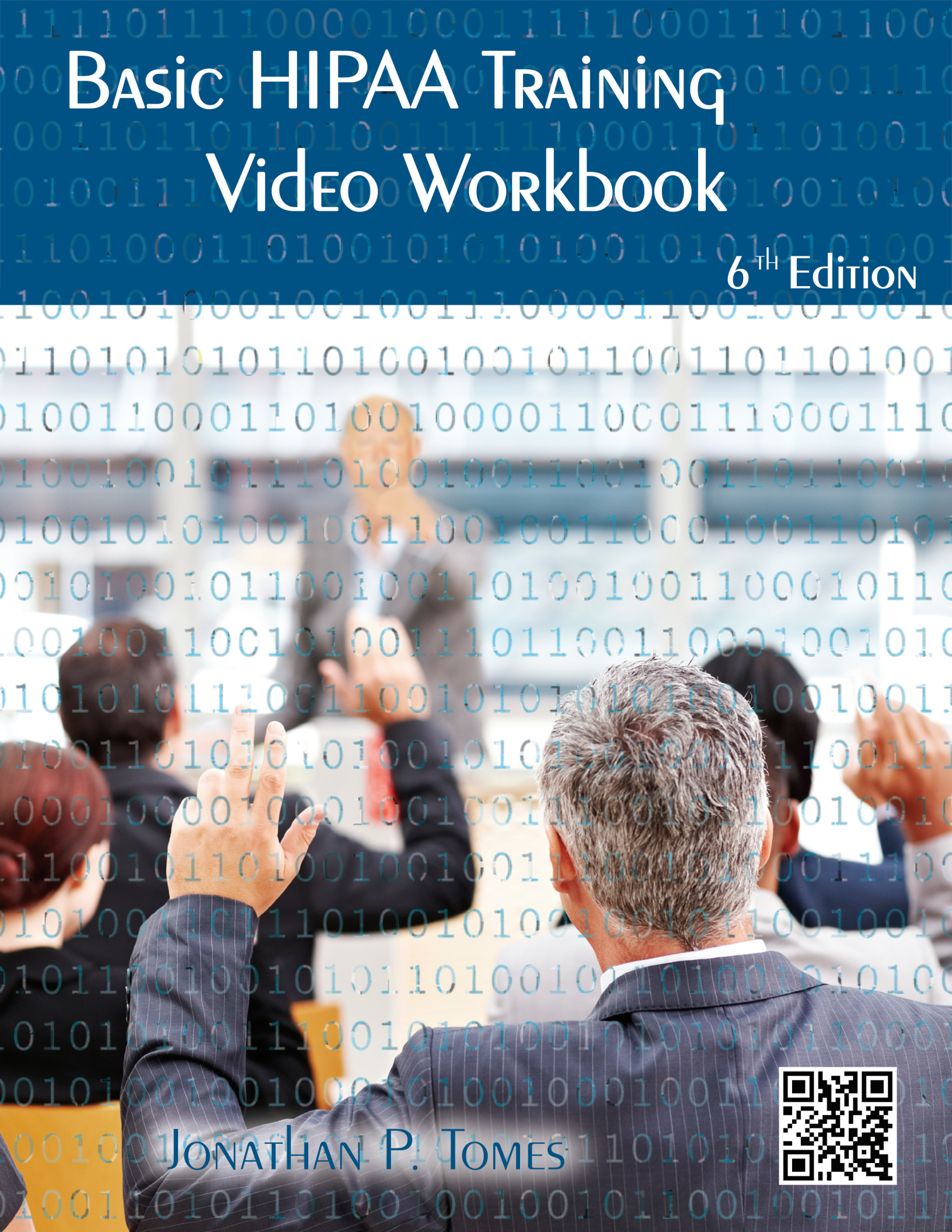
Basic HIPAA Training Video Workbook

6th Edition



Jonathan P. Tomes

Basic HIPAA Training Video Workbook

6th Edition

By Jonathan P. Tomes

VETERANS PRESS INC

Published by
Veterans Press, Inc.
7111 W. 98th Terrace, Suite 140
Overland Park, KS 66212
Phone 913.341.8783 or toll-free 855.341.8783
Fax 913.385.7997
Email hipaa@veteranspress.com
Website www.veteranspress.com

Printed in the United States of America

Sixth Edition

First Printing

22 21 20 19 18 17 16 15 14 13 10 9 8 7 6 5 4 3 2 1

ISBN 978-1-880483-66-4

Introduction

To provide effective treatment, health care providers must have comprehensive, accurate, and timely medical information. The automation of medical information permits the collection, analysis, storage, and retrieval of vast amounts of medical information that not only can be used, but also can be shared with other providers at remote locations. The increasing demand for access to medical information by providers and others, such as insurance companies, has led to increasing concern about patient privacy and confidentiality and has led to the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA requires providers and others who maintain health information to implement security measures to guard the integrity, confidentiality, and availability of patient information. HIPAA required Congress to enact a comprehensive patient confidentiality law. The Department of Health and Human Services ("DHHS") drafted its security regulations in 1998 and its privacy regulations in 1999. In December 2000, DHHS issued the final privacy regulations, which became final on April 14, 2001. The security regulations became final on April 20, 2003. Those who had to comply with HIPAA (covered entities) had two years from those dates to become compliant.

This course will help you to become familiar with HIPAA's requirements and your employer's expectations of you as a member of its workforce to comply with HIPAA and with your facility's policies and safeguards for the protection of patient information. It also serves as a HIPAA refresher course and an introduction to the new changes required by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and the so-called Omnibus Rule.[1]

What Is HIPAA?

HIPAA is a federal law. Congress enacted the "administrative simplification" section of HIPAA to streamline the claims process and to provide privacy and security for electronic health information.

In the Privacy Rule, DHHS broadened this protection to include all health information, regardless of form or format. Thus, the Privacy Rule applies every bit as much to paper records and oral communications containing individually identifiable health information (called protected health information or "PHI") as it does to electronic health information.

What Does HIPAA Have to Do with You?

Previous medical records confidentiality laws arguably applied only to practitioners and medical records professionals. HIPAA, however, clearly applies to all members of a health organization's workforce, from the chairman of the governing board all the way down to the custodial staff. HIPAA's requirements clearly include the entire clinical staff, the finance office, the administrative office, and any other employee or independent contractor that has access to PHI.

The HITECH Act expanded HIPAA's criminal liability to employees *and other individuals*. Thus, patients, students, volunteers, visitors, vendors, cleaning crew personnel, and the like all could be criminally liable for misusing individually identifiable health information.

And under the HITECH Act, HIPAA applies even more broadly—to business associates of covered entities. Business associates are persons or entities that perform a service for, or on behalf of, a covered entity that involves PHI. Examples include a transcription service, a billing company, a document storage company, and the like. Before the HITECH Act, business associates had to agree only by contract to implement reasonable and appropriate security measures to protect the data of their clients. Now, by law, they must, among other things, follow the Security Rule. And the Omnibus Rule made "downstream" business associates—subcontractors—business associates. Thus, a shredding service that shreds documents for a billing company (the upstream business associate) is also a business associate and faces the same liability as does the upstream business associate.

What Does HIPAA Mean by a Medical Record?

HIPAA defines health information as—

> any information, whether oral or recorded in any form or medium, that
> (A) is created or received by a health care provider,[2] health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;[3] and
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Thus, for HIPAA purposes, it is irrelevant whether the information is in the formal medical record or elsewhere.

Sometimes, HIPAA Calls It "Protected Health Information" or "PHI"

HIPAA broadened the previous definition of health information beyond the clinical to include financial, demographic, and lifestyle information maintained on patients and clients.

This information may be as sensitive as the clinical. In the first HIPAA criminal conviction, a patient accounts worker used financial and demographic information to obtain credit cards in a patient's name that the worker then ran up. As will be discussed below, the majority of the HIPAA convictions to date did not involve the clinical data, but rather the financial and demographic data—used for identity theft.

Thus, the covered entity—and now after the HITECH Act the business associate of a covered entity—that you work for has to protect all individually identifiable health information as defined above—not just the clinical. And so do you!

What Does "Protect Medical Information" Mean?

HIPAA requires you to protect the integrity, confidentiality, and availability of medical information. Integrity is a simple concept: the data is available when you need it, and it is accurate. Inaccurate or unavailable data can result in great harm, such as medical malpractice for administering too great a dose of the right drug or any dose of the wrong one, such as one that the client is allergic to.

What Is Confidentiality of Medical Information?

Synonyms of confidentiality are privacy and secrecy. No one should access, view, or disclose individually identifiable health information without a valid clinical, administrative, or business need to do so or unless the patient consents or the law requires the use or disclosure.

Before HIPAA, your facility likely already had a culture of protecting the confidentiality of very sensitive information, such as mental health and substance abuse information, so in one sense, HIPAA has not caused a big change. In another sense, HIPAA makes it clear that the culture of confidentiality must extend to everyone in the organization and that the facility must be able to prove that it complies with HIPAA. Further, the HITECH Act has now extended that requirement to business associates of covered entities.

What Could Happen If You Don't Protect That Information?

Violating HIPAA can result in civil penalties, such as civil money penalties (fines), and criminal penalties, such as fines and federal prison sentences.

The lowest level of HIPAA crime is a misdemeanor. A law has to provide for more than a year's imprisonment for a crime to be a felony. So simply accessing or disclosing PHI improperly is a misdemeanor and can result in imprisonment for up to one year.

The law does not require that you know that what you did was a crime—only that you knowingly, as opposed to accidently, did what you did. Remember that ignorance of the law is no excuse. The purpose of this HIPAA training workbook and the accompanying video is to help you not be ignorant of the law.

The second level is a felony. If, for example, you tell an employee of a health care provider that you are an auditor from the health department to get access to a patient's chart when you aren't from the health department and you aren't doing an audit, such a deception is what the law calls "false pretenses." This second level of HIPAA criminal liability makes one criminally liable for using false pretenses to obtain PHI.

And the Biggie!

HIPAA reserves the most serious criminal penalties for the misuse of individually identifiable health information for commercial advantage (such as marketing without following HIPAA's marketing rules), personal gain (such as identity theft), or malicious harm.

Committing identity theft would certainly be an example of misusing PHI for one's personal gain. Obtaining PHI to direct market a new drug or to steal patients from another practice would be for commercial advantage, which is also covered by the HIPAA "biggie." Finally, telling people that they had AIDS when they didn't after you had seen a lab report that they had taken an HIV test would be malicious harm and would also qualify the offender for the maximum penalty of up to 10 years' imprisonment and a $250,000 fine.

Most of the criminal convictions to date have been for the HIPAA "biggie." Most of them have involved financial gain—committing identity theft.

Some of the HIPAA Criminal Convictions to Date

Certainly, the federal government will have obtained more convictions by the time that you read this. U.S. Attorneys do not have difficulty proving a HIPAA violation. For the misdemeanor—the offense punishable by one year—all that the U.S. Attorney has to prove is that the offender improperly accessed individually identifiable health information. The ease of obtaining a HIPAA conviction is demonstrated by the fact that all of the individuals convicted to date, but for one, have pled guilty.

The Andrea Smith case is important. Although she avoided jail—she received probation and community service—her case illustrates what can happen when you simply tell a significant other or friend the funny thing that happened with a patient or client. You may think that, if you don't use the client's name, there is nothing wrong with telling the funny story. A doctor, however, lost her job and was fined for posting on Facebook how stupid her patient was. She thought it was not a violation because she hadn't used his name. But she used his condition and her treatment, both of which were very rare, and everyone knew whom she was talking about. HIPAA has a list of more than 20 identifiers, all of which must be removed for information to be de-identified.

Some More Convictions

The Arkansas case is interesting. Yes, the three defendants avoided jail time, but they now have a federal conviction for improperly accessing a deceased celebrity's chart. Yes, a deceased patient keeps his or her privacy rights after death. What are the employment possibilities for doctors or staff members with a federal conviction on their record?

Note that the UCLA Health System doctor didn't do anything evil with the PHI that he had improperly accessed. He didn't try to sell the PHI to the *National Enquirer*, which may have been interested in the data because it was the PHI of Leonardo

DiCaprio and Barbara Walters. But for simply accessing their charts without a valid clinical, administrative, or business need to do so, he ended up in federal prison.

What Else Could Happen If You Break the HIPAA Law?

Under HIPAA, all employers must have a sanction policy requiring employee discipline for breaches of HIPAA, the DHHS regulations implementing HIPAA, and their own policies and procedures implementing HIPAA. This sanction policy should contain a system of progressive discipline that may start out with a reprimand but that also would provide for termination in serious cases. Although such a discipline system is called progressive, an employer is not required to start out with a minor disciplinary action in every case. For a serious breach, it may discharge an employee immediately.

In addition, an employer may, in appropriate cases, contact law enforcement or any relevant professional licensure or disciplinary organizations and cooperate in any investigation that such agencies may undertake. Breach of confidentiality is a ground for professional discipline, including license revocation, in every clinical discipline.

The HITECH Act increased the civil penalties from $100 per violation to a maximum of $50,000 for violations caused by willful neglect that are not properly corrected. Not having adopted a HIPAA compliant sanction policy and/or not following it would be willful neglect.

Recent Civil Money Penalties

The DHHS Office of the Inspector General ("OIG") recently audited DHHS's HIPAA enforcement and found that it had not been enforcing HIPAA sufficiently. These increased civil money penalties and settlements demonstrate that DHHS got the message.

In addition to the fines, DHHS imposes corrective action plans ("CAPs") to prevent similar breaches. These plans can require the adoption of new policies, more training, and other compliance actions.

More Civil Money Penalties

See a common thread here? Most of the civil money penalties or settlements in lieu thereof involve failure to conduct a risk analysis, to perform required training, and to have adequate policies and procedures (which, of course, requires enforcement of the policies and security measures).

Although no civil money penalties have been imposed against workforce members of covered entities of business associates to date, it would not seem to help your chances for a raise or Christmas bonus if your employer is hit with a seven-figure fine. And those chances will certainly be wholly gone if your employer terminates you for causing the business to get fined.

So How Do You Avoid These Legal and Employment Hassles?

Most of HIPAA compliance is just good common sense. You already know when information that you hear or read or otherwise come in contact with at your facility is personal and confidential. Ask yourself whether you would want your doctor or counselor to be talking about your confidential health information if you were one of your employer's patients or clients.

Be Discreet and Keep Your Mouth Shut!

Far more breaches of confidentiality have occurred as a result of "loose lips" than for any other reason, such as hackers, viruses, poor locks on file cabinets, and the like.

Your employer may have excellent technical, physical, and personnel security, but you are the key link because the best firewall, encryption, locks, and alarm systems are of little good if you go to a party and discuss your employer's PHI with unauthorized personnel—or even if such personnel overhear you talking with authorized personnel.

Although the first HIPAA convictions involved more than just improper access, such as using that access to commit identity theft, a number of the more recent convictions involve nothing more than improperly accessing a chart out of curiosity about a patient. HIPAA requires your employer to audit for improper access or use.

In the Andrea Smith HIPAA criminal case mentioned above, a nurse's act of telling her spouse about a patient resulted in the nurse pleading guilty, having to perform two years of community service, and being on probation for two years. The spouse called the patient up and threatened to use the PHI against the patient in a lawsuit. And now, after the HITECH Act's addition of "other individuals" to the list of those subject to HIPAA's criminal penalties, the spouse could be prosecuted, too.

Although telling your spouse, significant other, or friends about the amusing thing that happened at your facility concerning a patient or a client might be fun at the time, the consequences—your termination and perhaps other, worse penalties—would not be funny.

You might be able to avoid a HIPAA violation by not mentioning the patient or client's name, but why take the chance that some listener can put two and two together and figure out who the patient or client is?

Observe the "Need-to-Know" Rule

HIPAA and your employer require access authorization and policies governing access authorization. Under these required policies, workers may not have any more access to PHI than is necessary to perform their duties. These policies govern how your employer establishes access, modifies access, and terminates access. Your employer reserves the right to audit access to ensure compliance with its access policies.

Observe the "Need-to-Know" Rule

Yes, we are being redundant. But improper access is the leading cause of HIPAA violations. And we've seen what it can cost.

Use and Disclose Information Only as Permitted by Law and Company Policy

Another name for the "need-to-know" principle is the business or medical necessity rule. For the use or disclosure of patient or client PHI to be proper, a business or medical necessity must exist.

In addition, HIPAA also has a "minimum necessary" rule, under which employees are supposed to use or disclose only the minimum necessary PHI to do whatever they are doing. The minimum necessary rule does not, however, apply to the clinical setting because DHHS does not want to harm client care by specifying what the minimum necessary information is to care for clients. Those decisions are properly for the clinician to make.

HIPAA requires health care employers to adopt and enforce a number of policies, such as the sanction policy and the access policy already mentioned herein. The best way for you to avoid a HIPAA violation and its consequences, such as employee discipline, is to become very familiar with your employer's policies and to follow them strictly.

Security Rule

The Privacy Rule is more focused on patient and client rights to control the uses and disclosures of PHI while the Security Rule specifies how covered entities and now business associates of covered entities must protect electronic PHI ("EPHI").

DHHS and the (Finally) Final Security Regulations

The Security Rule covers data stored in a data repository or transmitted over a network. "Stored in a data repository" is very broadly defined to include a facility that is all paper, but that has a physician bring his laptop in to type his discharge summaries and then print them out to be put into the paper chart. The laptop—with its hard drive—is a data repository. So is a memory stick or a cell phone.

"Transmitted over any network" is even more broadly defined to include taking a memory stick or other device out of a port in one computer and physically carrying it over to another computer and inserting it into a port in that other computer, or the so-called transfer by sneakerware. Although such transfers are not within the computer definition of a network transmission, HIPAA uses this much broader definition.

Applicability

The Security Rule applies only to EPHI—electronic PHI. The Privacy Rule, however, requires reasonable and appropriate security measures for all PHI, not just EPHI.

Four Categories of Security Requirements

The four categories of security requirements are fairly self-explanatory. The general rules specify what covered entities must do to protect EPHI. The administrative safeguards category covers such things as the required policies and procedures. Physical safeguards have standards for the physical protection of electronic equipment and media, and technical safeguards have the same for technical protections, such as encryption.

General Provisions, § 164.306(a)

This part of the general provisions merely repeats the requirements of the HIPAA statute, adding the final bullet that a covered entity cannot escape the requirements of the rule by not transmitting any PHI outside the entity in electronic format.

Although the HIPAA statute speaks of ensuring compliance by officers and employees, the Security Rule changes this language to "workforce," which certainly not only includes officers and employees but also covers independent contractors, students, and even volunteers who have access to PHI.

Flexibility of Approach, § 164.306(b)

HIPAA is technologically neutral. It does not specify what, for example, virus protection software your employer must use. Rather, HIPAA requires your employer to protect EPHI from viruses but allows your employer to use any security measure that it believes will reasonably and appropriately accomplish such protection.

Factors to Consider in Deciding Which Security Measures to Use

HIPAA does not require the best available security measures, just reasonable and appropriate ones. In determining which measures are reasonable and appropriate, your employer considers its size, the complexity of its operations, its capabilities, its existing information infrastructure, the costs of security measures, and, most importantly, the threats that exist to its PHI. It quantifies those risks—how likely they are to occur and how harmful they would be if they did occur. Security measures focus on the big threats, those that are likely to occur and that would cause a big problem if they did.

Administrative Safeguards

These administrative safeguards require covered entities to adopt a number of policies and procedures to control the behavior of their workforce with regard to PHI.

Security Management Process

Covered entities (and now presumably business associates of covered entities should) must perform risk analysis to identify risks to PHI and to quantify those risks (how likely they are to occur and how harmful they would be if they did occur) and then select security measures to guard against those risks. Many of those security measures are specified in the policies adopted as a result of the risk analysis. Of course, doing so is of little help unless you implement the security measures that the risk analysis identifies as necessary.

Security Management Process Implementation Specifications

The sanction policy is probably the most important HIPAA policy because it is the document that puts the "teeth" into all of the other policies and procedures.

Information system activity review is nothing more than required auditing of use and disclosure of EPHI to ensure compliance with your employer's policies and procedures. HIPAA does not specify what your employer must audit for. Rather, your employer will decide what to audit for when performing risk analysis. Auditing for proper access is a must. Did the data user have a proper clinical, business, or administrative reason for the access?

Assigned Security Responsibility

Covered entities must appoint a Security Officer. You must know who the Security Officer is. He or she is responsible for overseeing the security of EPHI. The Privacy Officer is responsible for ensuring compliance with the Privacy Rule.

Workforce Security

Because most breaches of confidentiality are not the result of poor physical security or poor technical security, but rather the result of poor personnel security, HIPAA requires workforce security to ensure that only those workforce members who need access to EPHI have it. And personnel should be screened to determine whether any grounds exist that would indicate that they could not be trusted with confidential health or financial information.

Information Access Management

Your employer must have access policies and also a termination policy that specifies the steps to take to end the access of a workforce member who is leaving the job. Remember that the duty to protect confidentiality survives the ending of the employment relationship!

Security Awareness and Training

This HIPAA requirement is the reason that you are here. Your employer will determine what topics need refresher training and when that training will occur. It is critical that you pay attention and assimilate the training!

Security Incident Reporting

Reporting refers to the duty of **all** workforce members to report actual and suspected breaches. The response procedure specifies what happens when your employer receives such a report. Your employer must mitigate security breaches—that is, lessen the harm of the breach. For example, it might try to recover a missent fax and ask the unauthorized recipient not to further disclose the information. Another aspect of mitigation is to take steps, such as disciplining the offender and/or revising a policy, so that the breach does not occur again. The HITECH Act requires reporting of breaches to DHHS and/or to the subject(s) of the breach in some circumstances. If in doubt, report the breach!

Contingency Plan

Recent events have taught us the importance of having our data backed up and knowing what to do in a disaster. HIPAA recognizes the importance of ensuring that PHI is available when needed by requiring a data backup plan and a disaster recovery plan. You must know your duties in the event of a disaster.

Contingency Plan Implementation Specifications

Not only must covered entities have policies and procedures for preventing loss of data and recovering from an emergency, but also they must test those procedures. Finding out during a power outage that an uninterruptible power source does not work is not helpful.

Evaluation

Just because your employer has complied with the Privacy and Security Rules doesn't mean that it is done with HIPAA. It must stay compliant. Threats

change, technology changes, clinical operations change, and so forth. Thus, HIPAA requires covered entities to review periodically their security measures to ensure that they are still reasonable and appropriate. If you see a risk that is not addressed properly or if something changes so that you are not certain that existing security measures are sufficient, you should notify your security officer.

Business Associate Contracts and Other Arrangements

HIPAA requires covered entities to ensure that people or organizations that perform services for them involving PHI safeguard it in transmission and on their end. Thus, before you hire someone, such as, for example, an outside transcription service, you must determine whether a HIPAA business associate contract is necessary.

As stated above, the HITECH Act extends the HIPAA civil and criminal penalties to business associates and requires them, by law, to comply with the Security Rule and to use and disclose PHI only in accordance with the Privacy Rule, among other requirements.

Physical Safeguards, § 164.310

The Security Rule has only four categories of physical safeguards. Notwithstanding the small number of standards, compared to the administrative safeguards, physical security measures can be very helpful and cost effective. If, for example, the unauthorized person who learned of a workforce member's password cannot get into the locked office to log on to the computer, the physical security measure—an access control—will have prevented a breach.

Facility Access Controls

A facility access controls policy and procedure would cover such things as who is responsible for locking doors, whether visitors must wear badges, and the like.

Workstation Use

A workstation use policy tells workforce members how to behave at their workstations. For example, must they log off when taking a break, or is a password-protected screen saver an adequate security measure?

Workstation Security

The workstation security measure governs, among others, how display screens are situated so that unauthorized personnel cannot view them and what, if any, physical barriers to access must be in place.

Device and Media Controls

HIPAA requires covered entities to control all devices and media that maintain or transmit EPHI, not just desk top computers and mainframes. Thus, your employer's policies govern how to secure laptops and other devices and CDs and other media. Most of the large civil money penalties have involved loss or theft of portable devices or media.

In addition, covered entities must ensure that all EPHI is destroyed in a manner that protects confidentiality. For example, you cannot just throw an old computer out on a trash heap so that an unauthorized person could retrieve PHI from it. Several covered entities have settled for seven figures for violating HIPAA by throwing paper PHI away in a dumpster instead of shredding or otherwise properly disposing of it.

Technical Safeguards

These five technical safeguards may seem redundant with some of the administrative safeguards. These technical safeguards, however, are how your facility implements its access policy and its information system activity review (audit).

Access control covers how you technically limit access to those persons to whom your supervisors have given access under the access policies in your administrative safeguards.

Audit control determines how you technically perform the audit that you decided that you needed to do in your information system activity review.

Integrity means that the data is not improperly modified or deleted. You can (and should) correct inaccurate data, but it would be illegal, for example, to change a medical record to hide malpractice.

Person or entity authentication means that, through some combination of unique user identification and password or retinal scan or thumbprint reader, you can tell who accessed or manipulated the data.

Transmission security covers methods to ensure that data is not improperly modified or lost during transmission.

So What Do You Have to Do to Comply with the Security Rule?

Talk about redundant—we have certainly made all of these points before. But they bear repeating because they are so critical to HIPAA compliance and your duty to protect the confidentiality of patient and client information.

Note that we keep repeating the importance of following your organization's policies. But following your organization's policies is not all that you need to do. You need to be proactive, look for security risks and take action if you see one, and certainly take action if you suspect a breach of security or privacy.

Pay Attention during HIPAA Training

You are complying with HIPAA right now! You are attending required training. HIPAA requires initial training and periodic refresher training. It does not define "periodic," so your employer will decide when refresher training is needed.

Not only must you attend training, but also you must pay attention. No defense exists to a breach of confidentiality or of your employer's policies and procedures because you did not know what was expected of you because your employer has provided HIPAA compliant training for you.

Your employer may require you to sign a pledge that you have been trained, will follow its policies, and will comply with HIPAA and other federal and state laws protecting patient or client information.

And don't do anything to cause other workforce members not to take HIPAA training seriously. If they commit a HIPAA violation because they didn't pay attention because they thought that the training was no big deal, and it results in a breach, you may not be liable (unless you were their superior), but if the breach results in a seven-figure civil money penalty, there may be no money in the budget to give you a raise or a bonus.

Take Action When You Detect or Suspect a Breach!

When we talk about a breach, we are not just talking about an actual breach of confidentiality. We are also talking about a violation of a HIPAA rule or one of your employer's policies protecting PHI even if it does not result in a breach of confidentiality.

One could breach confidentiality in dozens of ways, all of which end up with an unauthorized person having access to PHI. Examples include overhearing a discussion about a patient or a client, an employee telling an unauthorized person something about a well-known patient or client, or another unauthorized entity or person receiving a fax containing PHI.

An actual breach of confidentiality is usually also a breach of a HIPAA rule and/or your employer's policy.

What action should you take? Proper actions could include immediate remedial action, such as telling the person discussing individually identifiable health information to shut up. Or turning off the screen when a person forgets to log off when leaving the workstation. Or reporting the matter to the security officer or your supervisor. And don't forget to follow your organization's report procedure.

HITECH Act Breach Definition

This new definition in the HITECH Act should actually help you. In the past, some covered entities thought that accidentally faxing a progress note to the wrong doctor or accidentally accessing the wrong chart was a HIPAA violation. Now, if done accidentally and in good faith as a part of your duties, it is not a HIPAA violation. But you should follow your report and response procedure so that the incident can be investigated and any necessary mitigation taken so that it does not recur.

Again, Take Action When You Detect or Suspect a Breach!

Again we are being redundant. But taking action when a breach or potential breach exists is crucial and worth beating you about the head and shoulders about. HIPAA and your employer's policies require you to take action when you actually detect or even merely suspect a breach—either of confidentiality or of your employer's policies and procedures. The action that you take may be as simple as turning off a computer screen when you notice that the user forgot to log off. By taking immediate action, you may prevent a breach of a policy turning into a breach of confidentiality that could cost one of your coworkers his or her job and that could cause your employer to have to face a government investigation.

Take Corrective Action

Failure to take corrective action is every bit as much a breach of HIPAA and your employer's policies as is the actual breach that you failed to correct. Report the breach to your superior or to the security or privacy officer as required by your employer's report/response policy. But even before you report it, consider whether you should take any other immediate action to contain the breach so that it doesn't get any worse, such as by telling the workforce member with loose lips to button it.

If you don't take action, both you and the person who committed the breach may face employee discipline, and that situation helps no one. Rather, if you stop the breach before it gets worse, you may help your coworker by keeping the discipline much less severe than if the breach had gotten out of hand and resulted in a serious breach of confidentiality.

Taking corrective action is even more important after the HITECH Act, which increases the fines for breaches that are not properly corrected. Corrective action includes such things as minimizing the breach, so that it doesn't get any worse, notifying the subject(s) of the breach so that they can take steps to protect themselves, tightening up security so that it doesn't happen again, and disciplining the person causing the breach if appropriate.

Know How to Report!

HIPAA contains "whistleblower protection." Under this protection, in its simplest terms, people that report a HIPAA violation in good faith cannot have any adverse action taken against them.

HIPAA requires reporting any and all suspected or actual breaches of confidentiality or your employer's policies and procedures. Failure to report may result in disciplinary action.

The first person to whom you should report a breach is your immediate supervisor. If he or she is not available, you should report to the privacy or the security officer as specified in your employer's report/response procedure. You should not report to DHHS without first making every effort to report to an official of your company.

Use Good Common Sense!

We keep returning to using your good common sense. You would not have been hired by a health care provider or insurer unless you had both intelligence and common sense. Use them!

Use Good Common Sense!

Your supervisor will welcome your questions about what is proper under HIPAA. Supervisors also face HIPAA's criminal penalties, and they certainly don't want to go to jail for a breach by one of their workers. If your supervisor can't or won't answer the question, go to the privacy and/or security officer.

Conclusion

Remember to familiarize yourself with *all* of your employer's policies and procedures protecting confidentiality. If you keep the principles of this training in mind, you should have little trouble both staying HIPAA compliant and protecting patients' or clients' confidential health information. And always use your good common sense. Good luck!

NOTES

[1] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, *Federal Register,* Vol. 78, No. 17, Friday, January 25, 2013, Rules and Regulations, pp. 5566 *et seq.*

[2] "Healthcare providers include a provider of services[,] . . . a provider of medical or other health services, and any other person furnishing health care services or supplies." § 1320(d)(3).

[3] "A healthcare clearinghouse is a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." § 1320(d)(1)(a).

About the Author

Jonathan P. Tomes is a health care attorney practicing in the greater Kansas City area. As a nationally recognized authority on the legal requirements for medical information, he is the author of *The Compliance Guide to HIPAA and the DHHS Regulations* and its accompanying *HIPAA Documents Resource Center CD* of sample policies, procedures, and contracts, both now in their 5th edition (6th edition forthcoming). He has also written *Electronic Health Records: A Practical Compliance Guide*, now in its 3rd edition, *Medical Records Retention Guide*, now in its 4th edition, *How to Handle HIPAA Breaches, Complaints, and Investigations: Everything You Need to Know, Have You Heard about HIPAA? A Practical HIPAA Compliance Guide for Audiologists and Speech Pathologists, Mental and Behavioral Health and HIPAA: An Uneasy Alliance,* and most recently *The Complete HIPAA Policies and Procedures Guide* with accompanying *HIPAA Compliance Sample Policies and Procedures CD,* among more than 50 other books. His articles have appeared in *Health Data Management, Medical Claims Management, Credit Card Management, Journal of the Healthcare Financial Management Association, Journal of Health Care Finance, ACCA Docket,* and *Journal of AHIMA,* among others. Jon is a skilled attorney, having litigated hundreds of cases, including medical malpractice, Public Health Service disciplinary actions, Merit Systems Protection Board cases, physician disciplinary matters, Military Claims Act and Federal Tort Claims Act cases, and criminal cases. He has presented programs for AHIMA, Faulkner & Gray, HFMA, the American Bar Association, the American Society of Association Executives, the Business Network, state American Health Information Management Association chapters, Cross Country Education, and Lorman Business Centers.

Jon has also served as an expert witness in HIPAA and medical records cases.

Jon is a member of the editorial board of the *Journal of Health Care Finance* and the advisory board of *The Health Information Compliance Insider,* was the editor of *HIPAA & the HHS Regulation Compliance Quarterly,* and is a member of the American Health Lawyers Association and an associate member of the American Health Information Management Association. He is a member of the Illinois, Oklahoma, Kansas, and Missouri bars, the U.S. Supreme Court, the U.S. Court of Appeals for the Federal, 5th, 7th, 8th, and 10th Circuits, and the federal district courts for the Northern District of Illinois (trial bar), the District of Kansas, and the Western District of Missouri.

Jon's law firm, TOMES & DVORAK, CHARTERED, provides health law services, among others, including health information law, medical malpractice, representation before peer review and credentialing committees, fraud and abuse evaluation and defense, and legal review of managed care entities and operations.

Jon Tomes is also President of EMR Legal, a consulting firm that provides consulting services on HIPAA compliance and other issues regarding health information.

Jon is also President and Publisher of Veterans Press, Inc.

Jon also writes novels. *HIPAA Hysteria* and *JAGC-Off: A Politically Incorrect Memoir of the Real Judge Advocate General's Corps* are available both in trade paperback from Veterans Press and Amazon and on Kindle and Nook. *Lawful Orders* is available on Kindle. And he recently published his first vampire romance, *A Unit of Blood,* on Kindle. He is now working on the sequels to *HIPAA Hysteria* and *A Unit of Blood.*