HIPAA

PRIVACY
AND
SECURITY
TRAINING

A SHORT GUIDE
by Daniel J. Solove
Introduction

HIPAA has extensive training requirements, and they are often a source of many questions and confusion. To whom do they apply? What topics must be covered? How often must people be trained?

HIPAA only provides some of the answers to the questions above, and it leaves a lot unanswered. To complicate matters, HIPAA’s Privacy Rule and HIPAA’s Security Rule both have separate training requirements. See HIPAA Privacy Rule, 45 CFR § 164.530(b)(1); HIPAA Security Rule, 45 CFR § 164.308(a)(5).

I will walk through the HIPAA training requirements and explain what is required and what isn’t. I will also provide information about what many institutions do for HIPAA training and my thoughts about best practices.

What types of organizations must provide HIPAA training?

HIPAA requires that covered entities (CEs) and business associates (BAs) provide HIPAA training to members of their workforce who handle protected health information (PHI). This means administrative and clinical personnel need to be trained. Business associates — and any of their subcontractors — must have training. Basically, anyone who comes into contact with PHI must be trained.

How long must the training be?

HIPAA doesn’t specify any particular length for the training. A common mistake in training programs is that they are often too long and bombard people with information they don’t need. Very long training programs — ones that go on for 2+ hours — often backfire and result in people remembering less.

I recommend that training be anywhere from 20 to 40 minutes for privacy and 20 to 40 minutes for security. What matters more than time is the content of the training and how effectively and memorably the information is taught.

What topics must HIPAA privacy training cover?

The HIPAA Privacy Rule says that training must be “as necessary and appropriate for the members of the workforce to carry out their functions.” HIPAA thus doesn’t require that everyone be trained in the same way. The Privacy Rule doesn’t provide much further guidance on the specific topics that should be covered.
Many employees may have functions with only a limited involvement with patients or PHI. If an employee is not involved in providing notice to patients or in providing patients with access to their records, they don’t need training on these topics.

Common and important HIPAA privacy topics to train about include:

- identifying PHI
- the minimum necessary rule
- the rules about when and how PHI may be disclosed
- the importance of confidentiality
- avoiding snooping (even when one has access to PHI)
- the need to keep an accounting of disclosures.

Patient rights and authorization are important topics for many employees at CE, but employees at BA will rarely need to know these topics. Basic information about BA obligations is important for employees at BAs.

And training should also discuss the consequences of failing to follow the HIPAA Privacy Rule — how people can be victimized by medical identity theft, how people can lose trust, how organizations can be penalized by HHS and other regulators for violations, and how employees can be penalized too — by their organizations, by civil and criminal penalties under HIPAA, and by state law.

What topics must HIPAA security training cover?

The HIPAA Security Rule requires organizations to “Implement a security awareness and training program for all members of its workforce (including management).”

Organizations must implement: (1) “periodic security updates,” (2) “procedures for guarding against, detecting, and reporting malicious software,” (3) procedures for monitoring login-attempts and reporting discrepancies,” and (4) “procedures for creating, changing, and safeguarding passwords.”

HIPAA only specifies a few topics that need to be covered, which include malicious software, authentication, and passwords. I believe that a lot more is needed. People need to understand broadly that they play a big role in data security. People need to learn about social engineering, including phishing, the dangers from websites and email attachments, the use of portable devices, and what to do when something seems suspicious.

The HIPAA Privacy rule also contains security protections for regular PHI (the Security Rule only applies to e PHI). I think it is important to discuss security for physical records too, including proper document retention and destruction.

What else should HIPAA training cover?

Training should motivate, not just educate. It isn’t effective to just throw a bunch of do’s and don’ts at employees. They need to understand why the rules matter.

People should be taught that good privacy and security practices can help them personally too. These are things that can protect themselves and their families from harm.
It is also important to point out that HIPAA isn’t the only regulation that must be followed. In many cases, there are state laws that are stricter than HIPAA, and HIPAA does not preempt more protective state law. So employees must know that they need to pay attention to state law where relevant.

Among the most important things that HIPAA training should cover are: (1) contact the privacy or security officers with any questions or concerns; (2) report anything suspicious or any possible violation immediately. The more people ask and the sooner they report troublesome things, the better.

**How much should people be told about HIPAA?**

A lot of training spends a lot of time talking about HIPAA. It goes into a long discussion of the history of HIPAA’s passage and development. It quotes specific HIPAA language and provisions. In my opinion, this stuff is not necessary and is often a waste of people’s time to cover. It is interesting to HIPAA lawyers, but most people would rather watch paint dry or be poked by hot needles.

HIPAA itself states that the training is actually not about HIPAA but an organization’s “policies and procedures with respect to protected health information.” Of course, these policies and procedures are based on HIPAA, so the HIPAA rules must be covered. But HIPAA doesn’t require that people become experts on HIPAA. Instead, it requires that people understand what they are supposed to do and what they are not supposed to do.

To the extent that policies and procedures diverge from HIPAA (perhaps because of stricter state law requirements, or due to special additional requirements in certain contracts, or due to an organization’s own practices which might be stricter than HIPAA), employees should be trained about these divergences. Employees should be provided with an organization’s policies and procedures.

**How role-based should training be?**

I have seen effective programs that are highly role-based as well as ones that are more general. For all employees, there is a basic body of common information. For example: understand what PHI is, maintain confidentiality, don’t snoop, use the minimum necessary amount of information, ask questions when in doubt, report anything suspicious, etc. Information for specific roles can then be added on. Keep in mind that as training becomes more role-based it also becomes more challenging to administer.

An approach that has worked well at many organizations is a hub-and-spokes approach — a common course (the hub) with the key information that everyone should know and then spokes for various specific roles. What matters most is the overarching goal: People must know what they are supposed to do to protect PHI in their jobs.
Why should HIPAA training do more than just convey rules?

Far too often, training is so focused on saying the right things that it fails to get employees to do the right things.

Training must be understood. Information is worthless unless people understand it.

Training must be remembered. If people don’t remember the training, then what’s the point?

Training must be followed. Many incidents aren’t due to ignorance; they are due to people just not caring enough about doing the right thing. People are busy; things are hectic; and following HIPAA can be inconvenient and cumbersome at times. Training must make people care.

How often must HIPAA training be given?

The HIPAA Privacy Rule states that training must be provided to “each new member of the workforce within a reasonable period of time after the person joins the covered entity’s workforce” and to “each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures . . . within a reasonable period of time after the material change becomes effective.”

In practice, most organizations train all employees annually on HIPAA, and I strongly believe that this is the best practice. Memories fade quickly. Policies change and then the fact that these changes were made get forgotten. People need to be constantly reminded of what they must do because all it takes is one lapse and there will be an incident.

The HIPAA Security Rule requires periodic security updates. The Security Rule doesn’t define what “periodic” means. Nor does it define what the periodic security updates must consist of. The periodic updates can focus on a particular topic and they can be a module, a video, an email newsletter, a flyer, or anything else. I believe that short memorable messages spread out across the year can be immensely effective.

What are the consequences for inadequate HIPAA training?

There can be severe consequences:

First, HHS can issue a penalty of up to $1.5 million per provision of HIPAA violated. Inadequate training is low hanging fruit to OCR. The bottom line: Inadequate training = bigger fine!

Second, state attorneys general can enforce HIPAA too. Some state laws require training in HIPAA — you can be fined under Texas law up to $1.5 million for failing to follow HIPAA’s training requirement!

Third, because most privacy and security incidents involve human mistakes, training can reduce the risk of having such incidents.

Fourth, inadequate training can be flagged in a HIPAA audit if an organization is audited.
About the Author

Professor **Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world’s leading experts in privacy law, Solove has taught privacy and security law for 15 years, has published 10 books and more than 50 articles, including the leading textbook on privacy law and a short guidebook on the subject.

Professor Solove has spoken at hundreds of universities, federal agencies, and other organizations. He has given keynote addresses at many conferences, including one organized by the U.S. Department of Health and Human Services.

His LinkedIn blog has more than 1 million followers: [http://www.linkedin.com/today/post/articles/2259773](http://www.linkedin.com/today/post/articles/2259773)

Professor Solove organizes many events per year, including the Privacy + Security Forum, Oct. 4-6, 2017 in Washington, DC: [http://privacyandsecurityforum.com](http://privacyandsecurityforum.com)

About TeachPrivacy

TeachPrivacy was founded by Professor Daniel J. Solove. He is deeply involved in the creation of all training programs because he believes that training works best when made by subject-matter experts and by people with extensive teaching experience.

TeachPrivacy has a library of nearly 100 training courses that cover a wide array of privacy and security topics including HIPAA, FERPA, PCI, phishing, social engineering, and many others.

**Professor Solove’s HIPAA TRAINING**

<table>
<thead>
<tr>
<th>Drug Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Ingredients</strong></td>
</tr>
<tr>
<td>HIPAA expert + engaging teacher</td>
</tr>
<tr>
<td><strong>Effects</strong></td>
</tr>
<tr>
<td>• Lasting memory of key points</td>
</tr>
<tr>
<td>• Highly effective prevention of incidents</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
</tr>
<tr>
<td>So engaging that it is highly addictive.</td>
</tr>
</tbody>
</table>

[www.teachprivacy.com](http://www.teachprivacy.com)