HIPAA Security Rule

The HIPAA Security Rule, considered rather brief in terms of length and documentation for regulatory compliance legislation - nonetheless places a large focus on the protection of electronically Protected Health Information (ePHI). Ultimately, this requires covered entities, business associates, and any other relevant parties to have best-of-breed operational, business specific, and information security policies, procedures, and practices in place. While the HIPAA Security Rule technically includes parts 164.302 to 164.318, it's the Administrative, Physical, and Technical Safeguards that draw most attention - and rightfully so - as they provide explicit guidance on various mandates that must be in place for ensuring compliance.

HIPAA Security | 164.308 Administrative Safeguards

HIPAA 164.308 requires the following:

- Implement policies and procedures to prevent, detect, contain, and correct security violations.
- Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
- Implement policies and procedures to ensure that only appropriate members of the workforce have access to ePHI.
- Implement policies and procedures for authorized access to ePHI that are consistent with the applicable requirements of the PR.
- Implement a security awareness and training program for all members of its workforce (including management).
- Security incident procedures.
- Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that could damage systems that contain ePHI.
- Perform a periodic technical and non-technical evaluation to ensure that standards continue to be met in response to operational and environmental changes.
- Business associate contracts and other arrangements.

In summary, covered entities, business associates and other relevant parties are to have comprehensive policies and procedures in place addressing the aforementioned areas. As an employee of [company name], you have the right to request such documentation from authorized personnel for gaining a greater understanding of HIPAA 164.308 and general best practices relating to the protection of electronically Protected Health Information (ePHI).

HIPAA Security | 164.310 Physical Safeguards

HIPAA 164.310 requires the following:

- Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Workstation use.
- Workstation security.
- Device and media controls.

In summary, covered entities, business associates and other relevant parties are to have comprehensive policies and procedures in place addressing the aforementioned areas. As an employee of [company name], you have the right to request such documentation from authorized personnel for gaining a greater understanding of HIPAA 164.310 and general best practices relating to the protection of electronically Protected Health Information (ePHI). Note: You may notice the wording in HIPAA to be vague and general at times, what's important to note is that the aforementioned requirements are tailored to an organization's exact needs. Specifically, that means "policies and procedures" for a large, multi-chain health care provider would be vastly different for a small dentist office. HIPAA is also about scalability and flexibility, so please keep that in mind.

HIPAA Security | 164.312 Technical Safeguards

HIPAA 164.312 requires the following:

- Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have appropriately granted access rights.
- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
- Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

In summary, covered entities, business associates and other relevant parties are to have comprehensive policies and procedures in place addressing the aforementioned areas. As an employee of [company name], you have the right to request such documentation from authorized personnel for gaining a greater understanding of HIPAA 164.312 and general best practices relating to the protection of electronically Protected Health Information (ePHI). Note: 164.312 places a heavy emphasis on information security topic, for which you'll learn about throughout the HIPAA security awareness training material.

Laptop Security

Securing your laptop at all times is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, your laptop is a constant source of target, so beware. Take the following precautions for securing what's arguably one of your most important possessions:

- **Use Encryption.** The use of full-disk encryption ensures that safety and security of data (i.e., user files, swap files, system files, hidden files, etc.) residing on your laptop, especially if it's stolen, lost, or misplaced.

- **Use Anti-virus.** It's one of the most fundamentally important – and often not used – security software, so make sure your laptop has anti-virus running at all times, along with its scanning at regular intervals for viruses, and that the software is current.

- **Turn on your firewall.** Blocking suspicious traffic is essential for laptop security, so turn on and "enable" your default personal firewall or an approved personal firewall software appliance, for which there are many available

- **Use strong passwords.** When turning on your laptop, your initial password should be extremely strong, with a combination of letters, numbers, and symbols used. Once your initial password is compromised, the contents of your entire laptop (especially if you're not using full-disk encryption) can be compromised.

Don't use terms and phrases for which somebody might find an association with you, such as favorite football team, home address, middle name, etc.

- **It's your laptop.** Therefore, don't let other individuals use it, especially if it's somebody you don't know. When situations arise that require it to be used by someone other than you, create a guest account for their use.

- **Secure it physically.** A good investment is a security cable with a lock for securing your laptop at a workstation or any other location that requires such. They're relatively inexpensive and a great deterrent to any thief.

- **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe. That means not using the coffee house phrase "can you watch my laptop for a minute as I go to the restroom", or any other similar thought process. Being vigilant and watchful at all times is a must for the safety and security of your laptop, so remember – do not leave it unattended – plain and simple. If you have to leave in your hotel room or some other location, then remove it from sight and place under a pillow, in a closet, or some other location. The best safety measure is to carry it with you at all times.

- **Place your contact information somewhere visible.** Because most people are honest and trustworthy, should your laptop be stolen, misplaced or lost – and then subsequently found by a Good Samaritan – you'll clearly want your name, phone number, address, and/or email visible on it. Put a sticker on the cover or back of your laptop with all your relevant contact information.

- **And if your laptop is stolen.** Laptops unfortunately do get stolen, so think and act quickly, which means reporting the theft to local authorities along with informing management (and the I.T. department) immediately.

Software Licensing and Usage

It's also important to understand the company's general policy on software usage, which includes numerous responsibilities that all employees need to be aware of. Software is used by all of us, each and every day, as it's vital to performing daily tasks for one's job function. With that said, please be mindful of the following issues:

- **Use only approved software.** Only software approved and purchased from the company may be installed and used on any company-wide system components. This includes your workstation and any other device provided to you from the company. Unapproved software that has not been fully vetted by authorized I.T. personnel and can often contain dangerous or malicious code that's extremely harmful to computers. Simply stated, only load and use legally approved software on computers.

- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means you are not allowed to copy or duplicate any company approved and purchased software – no exceptions. U.S copyright laws – and other regulations throughout the world – often place strict guidelines on software usage, so please keep this in mind.

- **Use caution on your own devices.** When using your own personal workstation, laptop, or other device, please consider and be mindful of the software you install, especially when such computing systems are used for potentially accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, we still ask that you use extreme caution when loading any type of application onto your devices.

- **Accept updates.** For software to function efficiently and safely, security and patch updates have to be applied on a regular basis, so make sure to accept such updates when pushed out and also take time to update any software on your personal computers that do not rely on updates pushed out by I.T. personal.

- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements, and also comprehensively scanning the software for ensuring no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seem harmless, only to contain viruses that can wreak havoc on computers. Think before you start downloading any software online.

- **Software audits.** As an employee of the company, we have the right to conduct random software compliance audits on workstations, including laptops issued to you, or your own personal laptops. The audits are for ensuring compliance with software licensing rules, while also ensuring your computers are free of any potentially dangerous applications. If you're not sure what constitutes approved software, then simply ask somebody.

- **Penalties and fines.** Did you know that we as a company and you as an employee can actually be levied fines for improper software use? Yes, it's that serious and it's why we're taking the time to discuss this important issue with you. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages up to $150,000 (Section 504(c)(1) Title 17) per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to ten (Section 2319 (b) (2) Title 18) years.