HIPAA Compliance: Important Fundamentals You Need to Know

atlantic.net

Secure Cloud Services
Managed & Compliant Infrastructure

888-618-DATA (3282)
sales@atlantic.net
www.atlantic.net

Table of Contents

This e-book is essentially a Mega-Guide on HIPAA, the Health Insurance Portability and Accountability Act of 1996. First, we take a broad look at the basics of HIPAA; the roles of covered entities and business associates; and the related issue of HITECH compliance. Second, we discuss actionable steps to achieve compliance – closing with a straightforward and practical checklist.

Basics of HIPAA and HITECH

What exactly is HIPAA?

The **Health Insurance Portability and Accountability Act of 1996** is a US law that was passed to safeguard data and keep it from getting into the wrong hands. HIPAA became law when President Bill Clinton signed it in August 1996. Whether you agree with the regulations of HIPAA or not, well, they exist – and it can be expensive to your pocketbook and reputation to neglect them.

HIPAA (no, not HIPPA) is often discussed in tech circles for the obvious reason that hardware and software must keep digital patient information secured.

Here are the five components of this major healthcare act:

- **HIPAA Title I** makes it possible to maintain coverage when your employment changes and you're on a group plan. It also makes it unlawful for group insurance plans to turn down people they don't want to cover or to build lifetime maximums into contracts.
- **HIPAA Title II** "directs the U.S. Department of Health and Human Services to establish national standards for processing electronic healthcare transactions," explained Jacqueline Biscobing in *TechTarget*[1]. "It also requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS."
- **HIPAA Title III** introduces new tax rules related to healthcare treatment.
- **HIPAA Title IV** includes additional details on reform of insurance law, with protections for those who have pre-existing conditions and individuals who want to maintain their insurance.
- **HIPAA Title V** gives guidelines for life insurance policies that are owned by businesses and how to handle income tax specifics when

someone has their US citizenship revoked.

As you can see, the relevant section of HIPAA for IT providers, and for those processing, transferring, and/or storing health data, is Title II. This part of the law is often called simply the "Administrative Simplification provisions."

It establishes and describes these five elements:

- **National Provider Identifier Standard** – 10-digit NPI (national provider identifier) numbers must be assigned to all healthcare entities.

- **Transactions and Code Sets Standards** – An objectively approved protocol must be used in electronic data interchange (EDI).

- **HIPAA Privacy Rule** – Patient health information must be protected. "Privacy Rule" is actually shorthand for the "Standards for Privacy of Individually Identifiable Health Information."

- **HIPAA Security Rule** – This rule delineates expectations for the safeguarding of patient data. "Security Rule" is short for the "Security Standards for the Protection of Electronic Protected Health Information."

- **HIPAA Enforcement Rule** – This subsection of the law provides parameters with which companies should be investigated for potential or alleged violations.

Covered entities versus business associates

One of the most important elements of HIPAA is defining exactly what type of party is responsible for all its parameters – and that involves groups it describes as covered entities and business associates. Keep in mind that the distinction between these two parties is now less significant to healthcare law because the HIPAA Final Omnibus Rule moved to treat business associates as directly responsible for meeting all HIPAA requirements.

Nonetheless, by definition, a HIPAA covered entity is a healthcare plan, healthcare provider, or healthcare data clearinghouse that electronically sends and/or receives protected health information (PHI) as described by HIPAA and HHS standards. The transmission of PHI – or ePHI (electronic PHI) often occurs for one of two reasons: healthcare-related financial transactions and insurance processing, according to the HHS's *National Institutes of Health (NIH)*. "For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities," said the *NIH*. "Covered entities can be institutions, organizations, or persons."[2]

A HIPAA business associate is a person or organization that is not employed by a healthcare plan, provider, or clearinghouse, but that completes tasks related to individually identifiable health information, as governed by the HIPAA Administrative Simplification Rules (i.e. Title II, the crux of HIPAA compliance in an IT setting – see above), which includes the all-important Privacy Rule and Security Rule.

The HIPAA Omnibus Rule

A major change to the HIPAA rules came in January 2013[3], when the HHS announced its Omnibus Rule for HIPAA. This rule required that healthcare providers meet certain additional security requirements by September 23 of that same year[4]. (So that's been a few years ago whenever you're reading this, provided you don't have a time machine.)

A major specific change was to hit healthcare providers harder with penalties, raising the maximum fine for a single violation to $1.5 million (keeping in mind that's the maximum, depending on the degree of negligence).

HHS Secretary Kathleen Sebelius described the new rule in the agency's official announcement. "Much has changed in health care since HIPAA was enacted over fifteen years ago," she said. "The new rule will help protect patient privacy and safeguard patients' health information in an ever-expanding digital age."

Bear in mind that the specifics of the rule are beyond the scope of this e-book but are built into the tips and checklist for compliance below.

HITECH

HITECH is the acronym behind the Health Information Technology for Economic and Clinical Health Act of 2009. The legislation, signed into law by President Obama on February 17, was intended to accelerate the transition to electronic health records (EHR). It was actually included within the American Recovery and Reinvestment Act of 2009 (ARRA), which was geared toward stimulating the economy.

Another result of HITECH has to do with the Office of the National Coordinator for Health Information Technology (ONC), which has been part of the HHS Department since 2004. The ONC became responsible for administration and creation of standards related to HITECH.

"HITECH stipulated that, beginning in 2011, healthcare providers would be offered financial incentives for demonstrating 'meaningful use' of EHRs until 2015," noted Scot Petersen in *TechTarget*[5], "after which time penalties may be levied for failing to demonstrate such use."

As you can see, the HITECH law is geared more toward the adoption of electronic health records itself than it is toward specific security rules for digital data. That's why HIPAA is typically more a point of focus when looking for digital systems. However, many hosting providers and similar entities get certified for compliance with HITECH as well as HIPAA to demonstrate their knowledge of and

HIPAA Compliance Simplified

adherence to all federal healthcare law.

As you can imagine, there is overlap between these two laws. However, HITECH serves as somewhat of an addendum to HIPAA. It mandates that any standards for technology arising from HITECH must meet the HIPAA Privacy and Security Rules (described above).

Additionally, HIPAA states that healthcare providers must submit their systems to a HIPAA risk assessment in order to complete their meaningful use attestation – which is the healthcare provider confirming that they meaningfully use an EHR system.

Now that we know basically what we're talking about, let's go through important tips for compliance and actionable strategies – closing out with a HIPAA compliance checklist.

Five security-thought-leader tips for HIPAA compliance

Let's look first at some primary "legacy" advice on HIPAA in this section. The next section will get into some of the more recent rule changes. Then we'll provide a checklist that incorporates this advice into actionable steps so you can manage compliance simply and effectively.

Here are five core pieces of advice that relate to HIPAA before Final Omnibus, from Raj Chaudhary, who leads the security and privacy services group at consultancy *Crowe Horwath*[6]:

- **Keep data in the appropriate hands by strengthening security with logins.** "[L]et's make sure that when we assign user accounts to individuals that their role matches the access they are provided to the systems," said Chaudhary. "That is definitely one of the key elements of HIPAA – to make sure that only the people that need access to that information have a user ID or a user account." Also, for secure passwords,

require that new users have to switch any default ones and meet strict complexity guidelines. No-brainer, right?

- **Monitor controls and make sure logging is working correctly.** A key aspect of the HIPAA Security Rule is that you pay close attention to access of PHI. Simply put, you want to log everything. IT personnel should make sure that the logging feature is active within all systems around-the-clock. In addition to logging, you want to directly monitor via a system of rules, so you can examine your data accumulation process and be certain that everything is continually meeting your access controls.

- **Assess your access controls at all layers, including the network and your software.** At the level of the network, you have user IDs and strong passwords. This level of security is usually less problematic because it's managed directly by IT. The other critical layer, though, is the software, when anyone uses it. You need to maintain control of that layer.

Plus, although it's annoying to users to get locked out of their accounts, Chaudhary noted that it's a lesser evil to getting hacked. "[A]s an example, if somebody externally breaks in through your firewall to get to your systems and is now trying to guess the password, you've got to make sure that you have some sort of a lock-out after a few of these attempts," he said. "I typically recommend that after 10 failed attempts, one should be locked out."

- **Pay careful attention to your business associates who are handling any PHI, aka protected health information.** Chaudhury recommended carefully reviewing your business associate agreement (BAA) that controls your data relationship with each vendor who is handling your data. Note that as of the effective date of the Omnibus Rule (September 23, 2013), business associates now are directly responsible for meeting the parameters of HIPAA – in other

words, you are now less exposed by the law since the vendors carry some of the burden. Nonetheless, due diligence is still necessary.

His four step plan is:

1. Carefully read and sign a business associate agreement with the vendor.
2. Make sure you are in compliance with the "minimum necessary" protection. *To be clear, "minimum necessary" means that you only disclose the amount of information that you absolutely have to. It's an expectation set forth in the HIPAA Privacy Rule.*[7]
3. Conduct a performance assessment of the vendor.
4. Every year, reassess whether or not the business associate is in compliance with the BAA.

According to Chaudhary, covered entities (the healthcare plans, providers, and clearinghouses described above) often don't keep ongoing and updated records on their business associate agreements. "The agreements are not all consistent and not updated on a regular basis," he said. "And most likely, people don't apply the 'minimum necessary' rule and they provide more information than is necessary to perform that series of tasks that they were hired to do."

- **Create all-encompassing, step-by-step procedures for incident response and business continuity.** Basically, you need business continuity planning to be robust, and incident response planning needs to be fully described within your final documents. To manage business continuity, it's essential to conduct a business impact assessment, leading into a business continuity plan, and finishing out with a disaster recovery plan.

Chaudhary commented that one element of business continuity that is often neglected is the people. You need to know the people who are ultimately responsible to lead the response in the event of a disaster.

Also, when you are putting together the business impact assessment, keep in mind that your goal is to have

a reasonably good gauge of mission-critical systems – telling you the recovery time objectives that must be met in order to keep any expenses arising from a loss of business continuity to a minimum.

Three specific HIPAA tips you need to know post-omnibus

The Office for Civil Rights (OCR) of the HHS Department started performing HIPAA compliance audits more aggressively in 2016. Businesses are understandably concerned about audits because they don't want to end up in a publicity nightmare, with their competence and credibility called into question.

Prior to 2016, audits only occurred following a complaint or news report on problematic activity at a particular covered entity or business associate. A 2015 report found that the OCR was not doing enough to manage compliance with HIPAA. In 2016, the OCR "strengthen[ed] its review efforts by implementing a second phase of audits that was scheduled to occur in 2014, but encountered a number of delays," noted Clyde Bennett in *Help Net Security*[8]. For the assessments that took place in 2016, "providers with fewer than 15 physicians and healthcare business associates will be subject to audits," he added.

It's important to update your procedures and related documents so that you are up-to-date with HIPAA compliance following the adjustments made within the Final Omnibus Rule. Here are three basic considerations:

- **BAA 2.0** - You want your business associate agreement to reflect the Omnibus Rule, which broadened responsibility for HIPAA compliance to include business associates. It is now legally necessary for business associates to directly follow all HIPAA law.

- **Next-gen privacy policy** - Another big part of the Omnibus Rule was revisions of privacy parameters. Changes were made in treatment of deceased patients, patient access

rights, response to ePHI requests, disclosure to insurance and Medicare, data distribution, immunizations, and how to handle data for marketing, fundraising, and research purposes.

- **Forward-focused training** - Your staff needs to know how this critical healthcare law is changing, as indicated by the Omnibus Rule. Provide training to keep your business free of fines and lawsuits. Business associates need to train as well. Document this effort so you're audit-ready.

Checklist: How to Make Sure You're Compliant

The team at *HIPAA Journal*[9] went through the HIPAA Security, Privacy, and Breach Notification Rules; and the HIPAA Omnibus Rule to create this up-to-date checklist. What follows is a summary of the checklist, which is organized according to the various rules of HIPAA:

HIPAA Security Rule To-Do

Technical protections

- **Scramble**. Encrypt any ePHI to meet NIST parameters any time it is outside the firm's firewalled hardware. *(Must-do)*

- **Control access**. "This not only means assigning a centrally-controlled unique username and PIN code for each user," notes *HIPAA Journal*, "but also establishing procedures to govern the release or disclosure of ePHI during an emergency." *(Must-do)*

- **Authenticate ePHI**. You must authenticate because it protects data from corruption and incorrect destruction. *(Or alternatives)*

- **Become scramble-ready**. All devices that access the system should be able to encrypt and decrypt messages. *(Or alternatives)*

- **Control activity audits**. You want to log any access efforts and how data is manipulated. *(Must-do)*

- **Enable automatic logoff**. You log people out after a certain set timeframe. *(Or alternatives)*

Physical protections

- **Control facility access.** You want to carefully track the specific individuals who have physical access to data storage – not just engineers, but also repair people and even custodians. You must also take reason-

able steps to block unauthorized entry. *(Or alternatives)*

- **Manage workstations.** Write policy that limits which workstations can access health data, describes how a screen should be guarded from parties at a distance, and delineates proper workstation use. *(Must-do)*

- **Protect mobile.** You want a mobile device policy that removes data before a device is circulated to another user. *(Must-do)*

- **Track servers.** You want all your infrastructure in an inventory, along with information pertaining to where it's located. Copy all data completely before you move servers. *(Or alternatives)*

Administrative protections

- **Assess your risk.** Perform a comprehensive risk assessment for all health data. *(Must-do)*

- **Systematize risk management.** "The risk assessment must be repeated at regular intervals with measures introduced to reduce the risks to an appropriate level," advises *HIPAA Journal*. "A sanctions policy for employees who fail to comply with HIPAA regulations must also be introduced." *(Must-do)*

- **Train your staff.** You need to train on all ePHI access protocols and how to recognize potential hacking. Record all these sessions. *(Or alternatives)*

- **Build contingencies.** You must be able to achieve ongoing business continuity, responding to disasters with a prepared process that keeps data safe. *(Must-do)*

- **Test your contingencies.** You must test your contingency plan on a regular basis, with relation to all key software. A backup system and restoration policy should be adopted. *(Or alternatives)*

- **Block unauthorized access.** Be certain that parties that haven't been

granted access, such as subcontractors or parent companies, can't view ePHI. Sign business associate agreements with all partners. *(Must-do)*

- **Document all security incidents.** Note that this step is separate from the Breach Notification Rule, which has to do with actual successful hacks. A security incident can be stopped internally before data is breached. Staff should recognize and report these occurrences. *(Or alternatives)*

HIPAA Privacy Rule To-Do

- **Respond promptly.** HIPAA gives you 30 days to get back to patient access requests. *(Must-do)*

- **Get down with NPP.** Put together a
Notice of Privacy Practices (NPP) to officially inform patients and subscribers of data sharing policies. *(Must-do)*

- **Train your staff.** Beyond the training described above, make sure your personnel understand what data can and cannot be shared "beyond the firewall." *(Or alternatives)*

- **Don't succumb to corruption.** "Ensure appropriate steps are taken to maintain the integrity of ePHI and the individual personal identifiers of patients," instructs *HIPAA Journal*. *(Must-do)*

- **Get authority.** To have the authority to use ePHI for research, fundraising, or marketing, get permission from the patient. *(Must-do)*

- **Update your copy.** Your authorization forms should now include reference to changes in treatment of school immunizations, ePHI restriction in disclosure to health plans, and the right of patients to their electronic records. *(Must-do)*

HIPAA Breach Notification Rule To-Do

- **Let 'em know.** When a breach of ePHI occurs, you have to let both your patients and the HHS Depart-

ment know. If more than 500 people's records are involved, you also must notify the media. (Sound like fun?) Do you think you're off the hook if it's under 500 patients? Sorry, but no. You have to submit small-scale hacks through the OCR website. "These smaller breach reports should ideally be made once the initial investigation has been conducted," said *HIPAA Journal*. "The OCR only requires these reports to be made annually." All of the immediate notifications must be completed within 60 days post-discovery. *(Must-do)*

- **Check twice for four.** Make sure that your breach notification message contains these four elements: 1.) description of the ePHI and personal identifiers involved; 2.) what unauthorized party accessed it or related information; 3.) whether details were simply seen or taken – viewing vs. acquirement (if you know); and, 4.) the degree to which risk mitigation has succeeded. *(Must-do)*

HIPAA Omnibus Rule To-Do

Note: For space, this section will be abbreviated because it is covered, for the most part, above.

- **Refresh your BAA.** Update your Business Associate Agreements to reflect the language of the Omnibus Rule. *(Must-do)*

- **Send new BAA copies.** You have to get signed copies of a new BAA (with the Omnibus information incorporated) to stay compliant. *(Must-do)*

- **Revitalize your privacy policy.** Privacy policies must also reflect Omnibus changes. *(Must-do)*

- **Modernize your NPP.** "NPPs must be updated to cover the types of information that require an authorization, the right to opt out of correspondence for fundraising purposes and must factor in the new breach notification requirements," advised *HIPAA Journal*. *(Must-do)*

- **Finalize your training.** Make sure

that everyone on your staff is aware of all Omnibus Rule adjustments by conducting thorough training. (Or alternatives)

Our advice on the above steps, in terms of whatever you need to perform in-house, is it's a good idea to just do everything that's on the list – regardless of whether it's marked "Must-do" or "Or alternatives." After all, these designations are a bit unhelpful because you do still need to perform the step or a very similar alternative in order to be compliant. In the *HIPAA Journal* article, these items were called "Required" and "Addressable." "Even though privacy and security measures are referred to as 'addressable,' this does not mean they are optional," explained the publication. "Each of the criteria in our HIPAA compliance checklist has to be adhered to if your organization is to achieve full HIPAA compliance."

Get Help with HIPAA Compliance

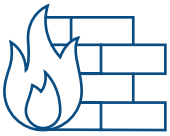
Hopefully the information and resources have been helpful. If you need help with HIPAA compliance, Atlantic.Net is here to help!

Atlantic.Net has been independently audited to meet all HIPAA compliance standards and requirements. Get a free consultation at 1.800.521.5881 or sales@atlantic.net. Visit https://www.atlantic.net/hipaa-compliant-hosting.

Atlantic.Net HIPAA Compliance Features

Business Associate Agreement

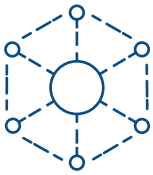
Intrusion Prevention System



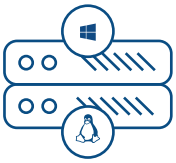
Fully Managed Firewall

Vulnerability Scans

Log Management System



Highly Available Bandwidth



Linux & Windows Servers

Encrypted Backup

File Integrity Monitoring

Antimalware Protection

Encrypted VPN

Encrypted Storage

References

[1] http://searchdatamanagement.techtarget.com/definition/HIPAA

[2] https://privacyruleandresearch.nih.gov/pr_06.asp

[3] http://www.hhs.gov/about/news/2013/01/17/new-rule-protects-patient-privacy-secures-health-information.html

[4] http://www.beckershospitalreview.com/legal-regulatory-issues/15-things-to-know-about-the-hipaa-omnibus-final-rulebefore-sept-23.html

[5] http://searchhealthit.techtarget.com/definition/HITECH-Act

[6] http://www.inforisktoday.com/interviews/five-hipaa-compliance-tips-i-981

[7] http://searchdatamanagement.techtarget.com/definition/HIPAA

[8] https://www.helpnetsecurity.com/2016/07/26/hipaa-complaint-2016-federal-changes/

[9] http://www.hipaajournal.com/hipaa-compliance-checklist/