RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

OnLINE TECH

UNDERSTAND BASICS AND BEST PRACTICES FOR HIPAA COMPLIANCE

RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

Are you wondering what all the HIPAA fuss is about? Here are a few basics go get you started, along with some reference to in-depth videos along the way.

WHAT IS HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996 that specifies laws for the protection and use of Personal (or Protected) Health Information (PHI) which is essentially your medical record. HIPAA was intended to ease the sharing of Personal Health Information (PHI) between entities that have a need to know while maintaining an acceptable and reasonable level of privacy to the individual whose information is at stake.

WHAT IS HITECH?

In 2010, the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed in order to update HIPAA rules and provided federal funds for deploying electronic medical records (EMR), also referred to as electronic health records (EHR). HITECH upgraded HIPAA because medical records were now in digital form, and as a result, they needed new rules for protection and availability.

WHAT DOES HIPAA COVER?

HIPAA covers the Privacy, Security and Enforcement rules of PHI. The Privacy and Security rules contain information on how one must treat PHI (whether it's electronic or not). The enforcement rules specify what happens if you don't (the penalties).

The 3 pillars of HIPAA are:

1. **Integrity of information** – the medical record must be accurate
2. **Confidentiality** – The medical record should only be seen by those with a need to know and all uses of that data should be knowable by the individual.
3. **Availability** – The medical record must be available, in essence, no reasonably avoidable downtime.

RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

WHO'S THE BOSS FOR THESE RULES? ARE THE HIPAA POLICE REAL?

The Acts are administered by the Department of Health and Human Services (HHS) in the Office of Civil Rights (OCR). It is the OCR which has the right to enforce, audit, fine and charge companies and individuals for violations of the Act. They interpret the law in the Act and write the rules and regulations.

WHAT ARE THE RULES AND REGULATIONS?

The rules and regulations are documented in the Code of Federal Regulations (CFR). Parts 160 and 164 of the CFR are the two that pertain to HIPAA. When someone says they adhere to HIPAA rules, it means they adhere to the paragraphs in the Parts. For example, one of the paragraphs says:

Paragraph 164.308(a)(1)(i) Standard: Security Management Practices – Implement policies and procedures to prevent, detect, contain, and correct security violations.

We are then required to do precisely what it says – prevent, detect, contain and correct security violations. At Online Tech, we have such a written policy and in that documented policy we reference this paragraph number. Note that these rules say nothing about how you achieve these objectives – that is what we decide and document in our policies.

WHAT DO THE RULES SAY WE MUST DO (AND NOT DO)?

Primarily:

- Protect the Availability, Integrity and Confidentiality of PHI
- Have Business Associates Agreements with any vendors that touch protected health information (PHI)
- Report any violations of PHI misuse to the OCR (yes, we actually must snitch if we see violations to the statutes).

They do not specify any specific technology platform or design, just that you must secure the data. There are industry best practices that they assume you would use, such as NIST for protecting data, or they would likely consider you negligent.

RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

WHAT ARE ALL THESE "SAFEGUARDS" ABOUT?

The requisite safeguards in the HIPAA Privacy and Security rules are divided into three different sections: Administrative, Physical, and Technical.

- Administrative safeguards are things like security training for all employees, or policies to never access client data.
- Physical security includes things like requiring two forms of authentication in order to open the doors in our data center. It might be a combination of a badge, fingerprint, pin code, or key fob – anything that requires at least 2 things to prove you are who you say you are.
- Technical security includes things like making sure that anti-virus software is on your server or using 2-factor authentication for remote VPN connections to a server.

WHAT ARE THE PENALTIES FOR VIOLATING HIPAA?

The penalties for violating HIPAA rules are severe and range from $100 to $50,000 per violation (or per record) up to a maximum of $1,500,000 per year and can carry criminal charges which could result in jail time. They are incurred if PHI (or ePHI, Electronic Personal Health Information) is released to the public in unencrypted form of more than 500 records.

Serious stuff. The fines and charges are broken down into 2 major categories: "Reasonable Cause" and "Willful Neglect".

- Reasonable Cause ranges from $100 to $50,000 per incident (release of 500 medical records) and does not involve any jail time.
- Willful Neglect ranges from $10,000 to $50,000 for each incident and can result in criminal charges.

RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

WHAT DOES IT MEAN TO HAVE A HIPAA AUDIT?

A HIPAA audit means that you have performed a diligent risk assessment against the latest OCR HIPAA Audit Protocol. Let's be honest: none of us can truly, objectively assess ourselves. Get an independent, third-party opinion or if you are working with a Business Associate and sharing protected health information (PHI), make sure to ask them for a copy of their independent assessment report. Then read it! You should see evidence of strong administrative, physical, and technical safeguards that protect patient information.

WHAT IS A BUSINESS ASSOCIATE (BA)?

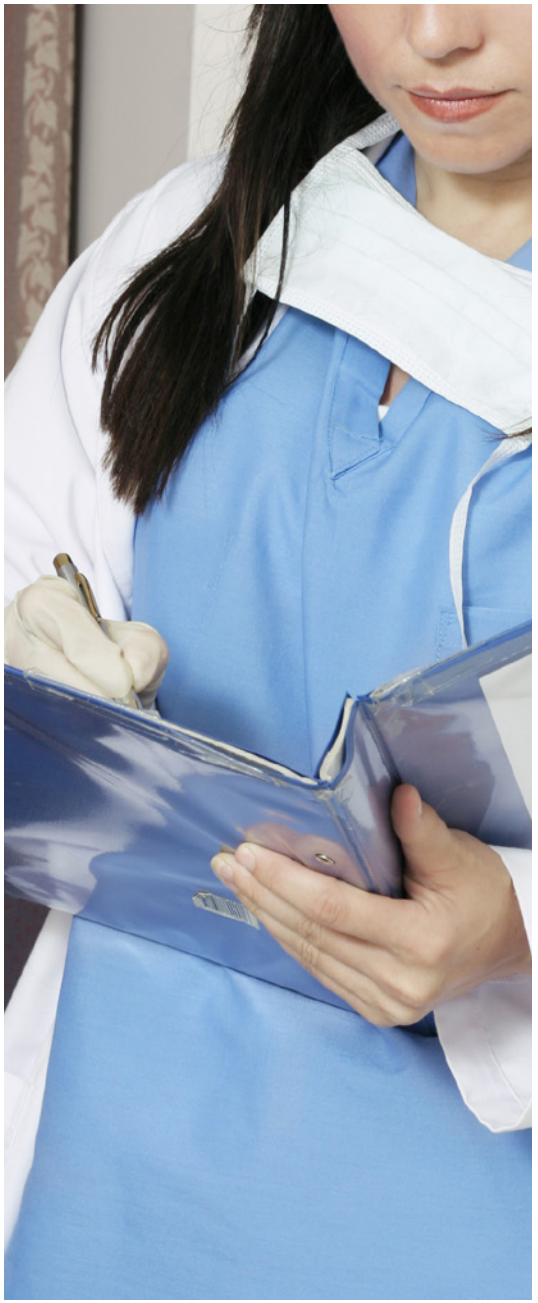
There are three types of entities described in the statute. The first is the patient. That's easy. The second is the Covered Entity (CE) and the third is the Business Associate (BA). The CE performs medical services on the patient and has the most trusted access of the information. A hospital or an insurance company is a CE.

A BA is someone contracted by a CE for services that involve the exchange of patient information (PHI). to perform the contracted service. A traditional BA is a bill processing company that sends medical invoices and processes payments. They have and need access to the patient information (name, address) and the medical record (diagnosis code, charge etc.) to perform the work for the CE.

IS MY BUSINESS CONSIDERED A BUSINESS ASSOCIATE?

If your company comes into contact with patient information, you are considered a Business Associate. At first, not everyone was convinced if cloud providers were indeed Business Associates until David S. Holtzman of the Health Information Privacy Division of OCR during a speech at the Health Care Compliance Association's 16th Annual Compliance Institute clarified:

"If you use a cloud service, it should be your business associate. If they refuse to sign a business associate agreement, don't use the cloud service"



RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

Another point they make is that business associates must also adhere to the Breach Notification Rule – including the subcontractors of business associates. Covered entities and business associates should take note – the document also states that "these proposed changes would make covered entities and business associates liable under § 160.402(c) for the acts of their business associate agents, in accordance 61 with the Federal common law of agency, regardless of whether the covered entity has a compliant business associate agreement in place."

WHEN IS A BAA REQUIRED?

A Business Associate Agreement is required whenever a client is storing, processing or transmitting protected health information (PHI).

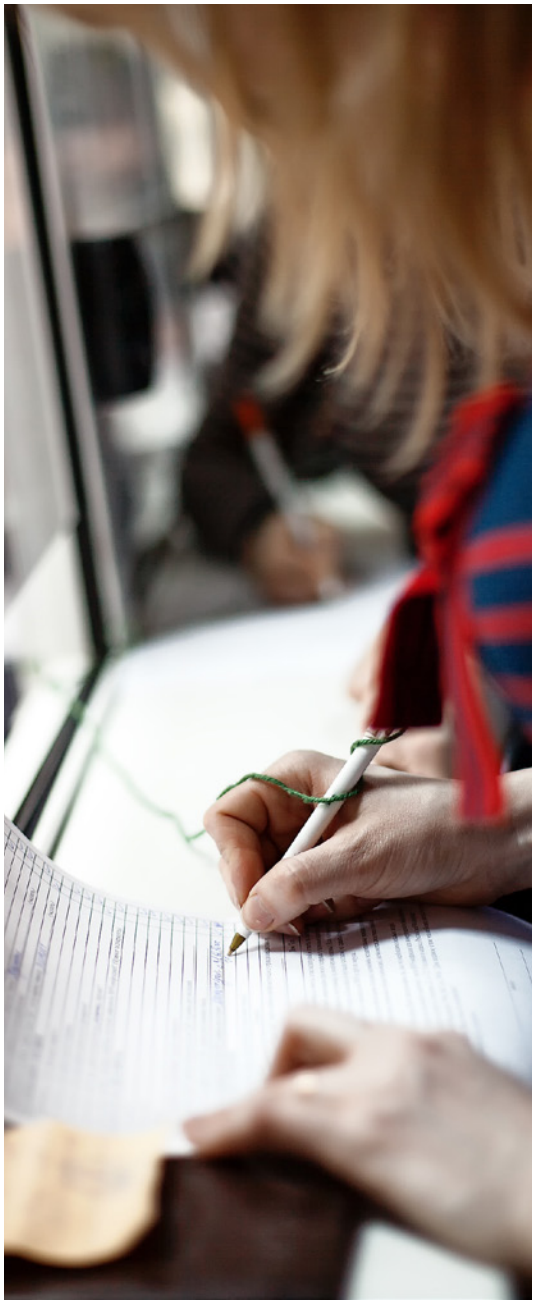
Does choosing a HIPAA compliant Business Associate make your business HIPAA compliant?

No. Every company must do their own risk assessment and mitigation planning that is specific to their own processes and procedures. That said, if you are working with a vendor who has performed the same level of due diligence, it saves you from having to spend a lot of time and money researching and detailing their protective practices to protect patient information. In our case, we provide all of our clients with our complete, independent HIPAA audit report. In turn, they can share this with their auditors to save time and money during their own audit.

WHAT ABOUT ENCRYPTION, IS IT REQUIRED?

Yes and no. Encryption is listed as "addressable" in the technical safeguards, instead of "required". Why? The healthcare information ecosystem is wildly diverse, and there are many different ways of protecting patient information. The easiest way to prove you meet this requirement, is to use AES 256 bit encryption on all data to the NIST standard. If you have adequately encrypted the data, then you are NOT required to report a data breach as long as the encryption keys have not been jeopardized and patient information remains safely encrypted.

If you opt not to use the recommended AES 256 encryption, it's on you to prove that your method is as good as, or better, than the NIST standard. If you can't prove that your protections meet or beat the NIST standard, you may be liable for penalties that fall into the expensive "negligent" category.



RAISE YOUR HIPAA IQ WITH A LITTLE FAQ

WHAT ARE SOME OTHER HIPAA BEST PRACTICES?

There are a few things that clients should do as it will help with their audit:

- Document data management, security, training and notification plans
- Client should use a Password policy for their access
- Encrypt PHI data whether it's in a database or in files on the server
- Do not use public FTP. Use other methods to move files
- Only use VPN access for remote access
- Login retry protection in their application
- Document a disaster recovery plan

ABOUT ONLINE TECH

Online Tech is the Midwest's leader in secure, compliant enterprise cloud and colocation hosting services. The company's network of five data centers protect mission critical applications to ensure they are always available, secure and comply with government and industry regulations. Backed by independent HIPAA, PCI, SSAE 16 and SOC 2 audits, Online Tech delivers exceptional experiences for companies in need of a strategic hosting partner.

For more information, call (877) 740-5028, email solutions@onlinetech.com or visit www.onlinetech.com.