

The 5 Things You Must Know About HIPAA

- **HIPAA** (Health Insurance Portability and Accountability Act of 1996) was created to help safeguard protected health information (PHI) from fraud and theft. Over the years HIPAA has evolved and is even more encompassing now, as well as becoming stricter. It is a difficult task to always maintain compliancy with the changes in technology. This is where we would like to step in and help.

What do you need to know?

- 1. Penalties Are Serious.
 - The cost of HIPAA fines has continued to rise over the last few years and shows no sign of slowing down, especially with OCR (Office of Civil Rights) wanting to crack down harder on healthcare facilities. With just 1 person's medical records being worth up to \$1,000 on the black market it should be no surprise that they want to do whatever they can to help secure PHI. It is easy to violate HIPAA if you aren't taking it seriously. If you are planning on being reactive and not proactive, you could end up finding yourself in hot water when an auditor comes knocking. The total for fines in 2015 equated to \$6,193,000 just 3 years later in 2018 they equated to \$28,683,400, over 4x the total fine cost of 2015. According to organization PCIHIPAA, the 2018 total of over \$28.5 million is expected to more than double by 2020.
- 2. An MSP is the Best Defense in the Case of an Audit.
 - A HIPAA audit is when a healthcare facility is inspected regarding compliancy with HIPAA rules and regulations. Whether you are a small or large organization it can be difficult to be completely prepared for an audit. An MSP will have many security measures in place and should be able to help present logs and reports for the auditor to examine regarding ePHI (electronic protected health information). One of the major benefits of these reports MSPs can generate is knowing who accessed certain files at a given time or who might have been remoting into the network and from what device.
- 3. You Need a BAA.
 - A Business Associate Agreement (BAA) is essentially a signed contract between a health care provider and an outside company that performs services in which the associate might come in contact with PHI. Common examples of such contractors are MSPs (Managed Service Provider), legal teams, or accountants. According to the Omnibus Rule introduced in 2013, HIPAA requires these agreements. If a person can potentially come in contact with PHI they are required to sign a BAA. It is better to lean on the safe side of if you think they may accidentally come in contact with PHI to have them sign a BAA. A great example of this is your IT, they typically will be well versed in your network and when they are working something on the network a PHI file may come across their screen.

OCR won't care if you aren't aware.

- 4. The Risk Assessment is Your Friend.
 - When it comes to HIPAA and compliancy knowledge is key. Being able to know and understand every single HIPAA regulation would be a near impossible task. This is where a risk assessment can be your savior. A risk assessment will be able to give you a detailed list of infractions your healthcare facility has. Not knowing or choosing to ignore HIPAA policies does not mean you are safe, this possibly puts you at an even higher risk of an audit which then leads to fines.
- 5. It pays to document.
 - According to Security Metrics, documentation is the failsafe that keeps your hands clean, keeps your company transparent, and keeps your security efforts organized. Not only do you have to ensure you have written policies and procedures in place, but you also have to train your staff thoroughly on them. Proper training is necessary for compliancy. Knowing that the correct policies, procedures, and training on them has taken place will help create a peace of mind during an audit. With a good MSP on your side they can help step in with documentation. Like stated earlier an MSP will be able to provide logs and reports of ePHI.

Why do you need to know about HIPAA?

- All companies, big or small, that deal with PHI are subject to an audit and need to know what that means. It's not a matter of if, but a matter of when you will be audited, and knowledge is key. Always being 100% ready for an audit seems like a large task to ask of a healthcare provider but this is made easier with a great MSP to help lean on.

What policies and procedures do you currently have in place?

- Policies and procedures are the most important documentation when it comes to HIPAA compliancy. Ensuring you have proper documentation in place can make the difference of receiving a hefty fine or successfully going through an audit. Like previously stated in section 5, a great MSP will be able to help provide logs and reports for the auditor to examine. Being able to present these files is a good example of a procedure that your MSP should be following.

Why should you care if you have a good MSP when it comes to IT?

- With technology continuing to evolve HIPAA has to evolve alongside it to help protect PHI. As technology grows it is becoming easier to fall out of compliancy due to a lack of knowledge of the technological advances you may need to maintain. With the right MSP they should be able to help you with making these decisions.

OCR won't care if you aren't aware.