What is HIPPA/PCI?

In this digital era, where every bit of information pertaining to individuals has gone digital and is stored in digital form somewhere or the other, there is a need protect the individuals from having their data exposed to unauthorised entities. With this view, there are a number of security and privacy regulations that have been prescribed by Law, as well as by certain industries; and compliance with these has to be ensured by all entities – whether they be organizations or individuals. HIPAA and PCI-DSS are two such regulations and standards that are the concern of CISOs today.

HIPAA and PCI DSS are both frameworks for complying with legal guidelines that ensure the underlying data is protected appropriately. Whereas HIPAA is focused on protecting Protected Health Information (PHI) or Electronic Health Records (EHR), PCI-DSS is centred around an individual's credit card data.

Compliance to both of these regulatory frameworks is essential, but the fact is that complying with one does not automatically mean compliance with the other. These are two different things, and organizations and individuals who are bound by these regulations are required to ensure careful adherence to both.

Since the subject is of considerable importance, let us examine HIPAA and PCI in a little more depth.

Understanding HIPAA

The US government enacted a law, way back in the year 1996. It was called HIPAA- short for Health Industry Portability and Accountability Act. This law covers, among other things, the protection of the privacy of individuals' health-related information.

To comply with HIPAA, the responsible organizations and individuals must adhere to certain strict guidelines and must take certain steps. And by 'responsible organizations and individuals' we mean healthcare providers, health plans, healthcare clearinghouses, as well as third parties and business associates handling patient health-related information.

We will look at the HIPAA requirements and rules, and what it takes to comply with them, a little later in this article.

Understanding PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that companies that accept, process, store or transmit credit card information maintain a secure environment. The PCI DSS is administered and managed by the PCI Security Standards Council, which is an independent body created by major payment card brands acting together.

The PCI DSS standards apply to merchants, and in general all entities that accept card payments. Accepting card payment entails accessing, storing and transmitting individuals' card data. PCI DSS applies to all companies that accept credit card payments.

PCI compliance encompasses a set of 12 requirements, aimed towards achieving certain security goals. We will look these requirements in more detail, later in this article.

What is expected out of organizations to ensure HIPPA/PCI compliance?

HIPAA Compliance

HIPAA compliance has been one of the major concern of healthcare IT leadership ever since the act was introduced way back in 1996, and the advent of high speed Internet access and mobility have only heightened the concerns. HIPAA is hard to interpret in an IT sense, because the language is a bit ambiguous. Let us look at how an organization can be HIPAA-compliant, in simplified terms.

HIPAA requires that the entities covered under HIPAA, and their business associates must ensure the privacy, security and availability of Protected Health Information (PHI) at all times.

To be compliant, there are four essential rules they must abide by. These rules are voluminous and complex, and we have tried to simplify the explanation to the barebones here. Further detailed reading can be obtained from the references listed at the end of this article.

Rule 1 HIPAA Privacy

This rule requires the entities and their business associates to put safeguards in place to protect patient health information.

Rule 2 HIPAA Security

This rule requires them to reasonably limit uses and sharing to the minimum necessary to accomplish your intended purpose.

Rule 3 HIPAA Enforcement

This rule requires the entities and their business associates to have agreements in place with any service providers that perform covered functions or activities for them. These agreements (BAAs) are to ensure that these services providers (Business Associates) only use and disclose patient health information properly and safeguard it appropriately.

Rule 4 HIPAA Breach Notification

This rule requires that they have procedures in place to limit who can access patient health information, and implement a training program for their employees about how to protect the patient health information.

PCI Compliance

The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

To be PCI DSS compliant, an organization has to meet a set of 12 requirements, as we mentioned earlier. These 12 requirements relate to a set of security goals. The security goals and the corresponding requirements are as follows:

Goal: Protect Cardholder Data

This goal is set to ensure that the cardholder data stored, accessed and transmitted by anyone is protected from exposure to unauthorised parties. Attaining this goal involves protecting the cardholder data stored in systems through muti-layered security systems, that include virtual security to control access to software systems as well as physical security which encompasses keeping the premises where the data is stored, and the access points, physically locked and secured. This additionally includes security for transmitted data-that, cardholder information that is transmitted across an open network like the Internet. Such data should never be transmitted in plaintext, but should be always encrypted using secure encryption algorithms.

An important tenet in attaining this goal is that cardholder data should be stored only on need basis. Sensitive information like PIN and CVV numbers should never be stored.

Goal: Maintaining a Vulnerability Management Program

Vulnerability Management refers to discovering and plugging points of insecurity, through which unauthorized access or damage can be caused to the systems hosting cardholder data. This goal is attained through maintaining systems that audit, discover and alert for vulnerabilities, and also by installing antivirus and anomaly detection systems that protect from malware.

Goal: Maintaining Strong Access Control Methods

Attaining this goal involves restricting user access to cardholder data, using unique IDs and secure authorization and authentication mechanisms, password encryption and expiry and other such measures. System access should be regularly tracked and monitored. Physical monitoring through surveillance cameras, restricting and logging all physical entry and access are also an important part of PCI compliance. This goal also includes scanning and testing for hidden vulnerabilities and taking action in case any vulnerabilities are uncovered.

Goal: Maintaining an Information Security Policy

According to standard definitions, an Information Security Policy is a set of rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. Attaining this goal involves setting up an Information Security Policy for the organization and ensuring its adherence. This policy should cover things like acceptable uses of technology, risk reviews at a senior level, operational security procedures, and other general administrative tasks.

What are the associated risks if you don't comply?

Non-Compliance to HIPAA

HIPAA non-compliances and violations are serious. They can result in various degrees of monetary penalties, and can even extend to imprisonment.

Wilful or intentional breaches are considered as criminal offenses and fall under the jurisdiction of the Department of Justice (DOJ)

The body responsible for enforcing HIPAA is the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)

In addition to the above penalties, the names of violators are put up in the 'name and shame' galleries of the OCR, and result in loss of image and trust.

PCI non-compliance

PCI is different from HIPAA in the sense that it is an industry standards requirement, and is not a law; whereas HIPAA is a law enacted by the US government.

Like HIPAA, PCI non-compliance can also result in fines and penalties, if the entity suffers a breach and is found to have not instituted PCI-compliance measures. The fines are actually enforced by the Payment Card brands. And the penalty is levied not on the violator, but on the violating entity's acquiring bank. The banks in turn, therefore set the rules that their merchants must follow, in order that they might avoid PCI- penalties.

These fines are different based on the degree of the non-compliance. Merchants might have to pay anywhere from $5,000 to $100,000 every month until they address all compliance issues. The bank or the payment card brand may revoke their ability to accept payments, if they don't resolve the issues in the agreed timeframes.

How does Seqrite help you comply with HIPPA/PCI?

Seqrite Endpoint Security (EPS) offers simplified endpoint security for multiple platforms and provides a centralized management solution that helps organizations to be compliant with HIPAA/PCI regulations by ensuring the required physical, technical safeguards are in place. Additionally, various features of Seqrite EPS is certified by prestigious certifications such as AVTest, AVLab and Checkmark.

Physical safeguards that EPS Seqrite offers:

- Advanced Device Control enables to enforce control over use of various physical devices within the network.

Network and transmission safeguards offered by Seqrite EPS

- Seqrite EPS Firewall Protection allows to block/allow inbound and outbound connections to certain ports/IP addresses.
- Seqrite EPS IDS/IPS feature helps to prevent intrusion attempts and port scanning attacks.

Technical safeguards offered by Seqrite EPS, Encryption:

- Seqrite EPS safeguards security and confidentiality of sensitive data. Data Loss Prevention (DLP) monitors data in motion as well as data at rest. DLP monitors confidential and sensitive information flowing out through various data transfer channels like Removable drives, Network shares, and through various applications like Chat Messengers, File sharing/Cloud services applications like Dropbox, etc. DLP monitors personal as well as health insurance information.
- Seqrite Encryption protects data by offering full disk encryption and removable disk encryption. It encrypts data with strong encryption algorithm and offers boot time authentication to restrict unauthorized access to endpoints.

- Vulnerability Scan feature gives detailed information about the known application vulnerabilities in the network. Patch Management feature helps to patch vulnerabilities by installing missing patches to make network more secure and less prone to security attacks.
- Application control in Seqrite EPS helps to enforce policies regarding use of various applications in the network. This prevents use of any unauthorized applications being used in the network.

Reporting in Seqrite EPS

- Seqrite EPS gives detailed reports of security and data leak incidences with all the necessary information that includes the data, time of incident and other incident details. With all this critical information, administrators can take necessary action and strengthen the safeguards in place.

Group policies enforcement features in Seqrite EPS

- Seqrite EPS policies can be customized are per requirement for various groups in the organization.

Quick Heal Technologies Limited
Corporate office: Marvel Edge, Office No. 7010 C & D, 7th Floor,
Viman Nagar, Pune - 411014, India.
Support Number: 1800-212-7377 | info@seqrite.com | www.seqrite.com