HIPAA

Why was HIPAA Created?

The Health Insurance Portability and Accountability Act (HIPAA) was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and to address limitations on healthcare insurance coverage – such as portability and the coverage of individuals with pre-existing conditions. Although responsible for widespread changes in the healthcare and healthcare insurance industries, the changes did not occur overnight. When the Act was passed in 1996, it only required the Secretary of Health and Human Services (HSS) to propose standards that would protect individually identifiable health information. The first set of proposed "Code Set" standards was not published until 1999, and the first proposals for the Privacy Rule only emerged in 2000. HIPAA legislation has evolved significantly since its earliest incarnation. Not only has the language of the Act been modified to address advances in technology, but the scope of the Act has been extended to cover Business Associates – third party service providers that perform a function on behalf of a HIPAA-Covered Entity that involves the use or disclosure of Protected Health Information (PHI). The HIPAA regulations are policed by the U.S. Department of Health & Human Services' Office for Civil Rights (OCR). State Attorneys General can also take action against Covered Entities and Business Associates found not to be in compliance with HIPAA. Both OCR and State Attorneys General have the authority to impose financial penalties on Covered Entities and Business Associates for violations of HIPAA.

What is the Purpose of HIPAA?

In addition to the original purpose of HIPAA, the way in which it is implemented is constantly changing to accommodate advances in technology and changes to working practices – both of which have resulted in new threats to patient privacy and the security of PHI. For example, the original HIPAA legislation was drafted eight years before Facebook came into existence and eleven years before the first iPhone was released. Therefore, since the original Privacy Rule, there have been a number of new HIPAA Rules (expanded on in the "HIPAA Explained" section below) plus frequent guidance has been issued by OCR regarding how Covered Entities and Business Associates should address issues such as BYOD policies, cloud computing and Workplace Wellness Programs. OCR guidance has also gone digital with the release of the Listserv application. Much of the original language of HIPAA has remained unaltered because, despite the changing technological landscape, it was written to cover a great number of diverse scenarios. Therefore, whether a Covered Entity is a medical center maintaining patient records or an insurance company transferring the healthcare rights of an individual who is changing jobs, the purpose of HIPAA remains the same as it did in 1996. HIPAA is also technology-neutral and does not favor one way of addressing a security vulnerability over another, provided the

mechanism introduced to correct a flaw or vulnerability is subjected to a risk assessment and the reason for implementing it in place of a specified measure is recorded. It is also important to note that HIPAA does not preempt state law, except in circumstances when a state's privacy and security regulations are weaker than those in HIPAA.

Understanding HIPAA

For the benefit of clarification, we have detailed below the eighteen personal identifiers that could allow a person to be identified. In the context of HIPAA for Dummies, when these personal identifiers are combined with health data the information is known as "Protected Health Information" or "PHI". When stored or communicated electronically, the acronym "PHI" is preceded by an "e" – i.e. "ePHI". Names or part of names Any other unique identifying characteristic Geographical identifiers Dates directly related to a person Phone number details Fax number details Details of Email addresses Social Security details Medical record numbers Health insurance beneficiary numbers Account details Certificate or license numbers Vehicle license plate details Device identifiers and serial numbers Website URLs IP address details Fingerprints, retinal and voice prints Complete face or any comparable photographic images The main takeaway for HIPAA compliance is that any company or individual that comes into contact with PHI must enact and enforce appropriate policies, procedures and safeguards to protect data.

HIPAA violations occur when there has been a failure to enact and enforce appropriate policies, procedures and safeguards, even when PHI has not been disclosed to or accessed by an unauthorized individual. Violations of HIPAA often result from the following: ♣ Lack of adequate risk analyses. ♣ Lack of comprehensive employee training. ♣ Inadequate Business Associate Agreements. ♣ Inappropriate disclosures of PHI. ♣ Ignorance of the minimum necessary rule. ♣ Failure to report breaches within the prescribed timeframe. Some HIPAA violations are accidental offences – for example, leaving a document containing PHI on a desk in clear view of anyone passing by. However, OCR does not consider ignorance an adequate excuse for HIPAA violations; and, although OCR may refrain from imposing a significant financial penalty on a Covered Entity for an accidental offence if the violation has not resulted in the unauthorized disclosure of PHI, it is likely that a course of "corrective action" will be required.

Who does HIPAA apply to?

Practically all health plans, healthcare clearinghouses, healthcare providers and endorsed sponsors of the Medicare prescription drug discount card are considered to be "HIPAA Covered Entities" (CEs) under the Act. Normally, these are entities that come into contact with PHI on a constant basis. Under the definition of HIPAA Covered Entities provided by HHS, most employers are not considered to be CEs, even if they maintain records of employees' health information. If employers use schemes such as the Employee Assistance Program (EAP), they

are then considered “hybrid entities” and are required to be HIPAAcompliant. “Business Associates” (BA) are also covered by HIPAA. These are entities who do not create, receive, manage or transmit PHI in the course of their main operations, but who supply services and perform certain functions for Covered Entities, during which they have access to PHI. Before undertaking a service or activity on behalf of a CE, a BA must complete a Business Associate Agreement guaranteeing to maintain the integrity of any PHI to which it has access, implement safeguards to protect the information, and restrict uses and disclosures of the information. HIPAA Rules Explained HIPAA legislation is essentially comprised of a number of rules, each of which lays out different requirements for HIPAA compliance. The rules are as follows: HIPAA Privacy Rule: The Privacy Rule dictates how, when and under what circumstances PHI can be used and disclosed. Enacted for the first time in 2003, it applies to all healthcare organizations, clearinghouses and entities that provide health plans. Since 2013, it has been extended to include Business Associates. The Privacy Rule sets limits regarding the use of patient information when no prior authorization has been given by the patient. Additionally, it mandates patients and their representatives have the right to obtain a copy of their health records and request corrections to errors. CEs have a 30-day deadline to respond to such requests. HIPAA Security Rule: The Security Rule sets the minimum standards to safeguard ePHI. Anybody within a CE or BA who can access, create, alter or transfer ePHI must follow these standards. Technical safeguards include encryption to NIST standards if the data goes outside the company’s firewall. Physical safeguards may relate to the layout of workstations (e.g. screens cannot be seen from a public area), whereas administrative safeguards unite the Privacy Rule and the Security Rule. They require a Security Officer and Privacy Officer to conduct regular risk assessments and audits. These assessments aim to identify any ways in which the integrity of PHI is threatened and build a risk management policy off the back of this.

Breach Notification Rule

The Department of Health and Human Services must be notified if a data breach has been discovered. This must be within 60 days of the breach’s discovery for incidents involving 500 or more individuals, and within 60 days of the end of the calendar year in which the breach was experienced for breaches of fewer than 500 records. Individuals whose personal information has been compromised must also be informed within 60 days, and if more than five hundred patients are affected in a particular jurisdiction, a media notice must be issued to a prominent news outlet serving that area.

Changes to the HIPAA Security Rule list the conditions (“safeguards”) that must be in place for HIPAA-compliant storage and the communication of ePHI. These “safeguards” are referred to in the HIPAA Security Rule as either “required” or “addressable”. In fact, all the security measures are generally required – irrespective of how they are listed – as the following section explains. The Required and Addressable Security Measures of HIPAA Explained One area of HIPAA that

has resulted in some confusion is the difference between “required” and “addressable” security measures. Practically every safeguard of HIPAA is “required” unless there is a justifiable rationale not to implement the safeguard, or an appropriate alternative to the safeguard is put in place that achieves the same objective and provides an equivalent level of protection. An instance in which the implementation of an addressable safeguard might be not required is the encryption of email. Emails containing ePHI – either in the body or as an attachment – only have to be encrypted if they are shared beyond a firewalled, internal server. If a healthcare group only uses email as an internal form of communication – or has an authorization from a patient to send their information unencrypted outside the protection of the firewall – there is no need to adopt this addressable safeguard. The decision not to use email encryption will have to be backed up by a risk assessment and must be documented in writing. Requirements HIPAA-covered entities are required to implement safeguards to ensure the confidentiality, integrity, and availability of ePHI. Arguably one of the most important safeguards is encryption, especially on portable devices such as laptop computers that are frequently taken off site.

HIPAA Password Requirements. HIPAA is vague when it comes to specific technologies and controls that should be applied to secure ePHI and systems that store health information, and this is certainly true for passwords. Even though passwords are one of the most basic safeguards to prevent unauthorized accessing of data and accounts, there is little mention of passwords in HIPAA. The only HIPAA password requirements that are specified are that HIPAA-covered entities and their business associates must implement “Procedures for creating, changing, and safeguarding passwords.” Even though password requirements are not detailed in HIPAA, HIPAA covered entities should develop policies covering the creation of passwords and base those policies on current best practices.

Highly complex passwords may be ‘more secure’ but they are difficult to remember. As a result, employees often write their passwords down. To avoid this, passwords should be difficult to guess but also memorable. The use of long passphrases rather than passwords is now recommended. Generally, passwords should: ♣ Be a minimum of 8 characters up to 64 characters, with passphrases – memorized secrets – longer than standard passwords recommended. ♣ NIST advises against storing password hints as these could be accessed by unauthorized individuals and be used to guess passwords. ♣ A password policy should be implemented to prevent commonly used weak passwords from being set, such as ‘password’, ‘12345678’, ‘letmein’ etc. ♣ NIST now recommends not forcing users to change their passwords frequently. A change should only be required infrequently or is there is very good reason for doing so – such as following a security breach. ♣ Multi-factor authentication should be implemented. ♣ NIST recommends salting and hashing stored passwords using a one-way key derivation function.

HIPAA Record Retention Requirements

There are no HIPAA record retention requirements as far as medical records are concerned but medical record retention requirements are covered by state laws. Data retention policies must therefore be developed accordingly. For instance, a hospital in the state of South Carolina must retain medical records for 11 years after the discharge date, while in Florida medical records must be retained by physicians for five years after the last patient contact and hospitals must retain medical records for seven years after the discharge date. When medical records are retained, they must be kept secure at all times.

HIPAA Violation Reporting Requirements The HIPAA Breach Notification Rule – 45 CFR §§ 164.400-414 – requires notifications to be issued after a breach of unsecured protected health information. A breach is defined as a use or disclosure of protected health information not permitted by the HIPAA Privacy Rule that compromises the security or privacy of protected health information. Notifications are not required if a HIPAA-covered entity or business associate can demonstrate there is a low probability that PHI has been compromised, with that determination made through a risk analysis.

If notifications are required, they must be issued to patients/health plan members 'without unnecessary delay' and no later than 60 days after the discovery of a breach. A media notice must also be issued if the breach impacts more than 500 individuals, again within 60 days. The notice should be provided to a prominent media outlet in the state or jurisdiction where the breach victims are located. The individual and media notices should include a brief description of the security breach, the types of information exposed, a brief description of what is being done by the breached entity to mitigate harm and prevent future breaches, and the steps that can be taken by breach victims to reduce the potential for harm.

Ten of the most common HIPAA violations.

These violations have been discovered by OCR during investigations of data breaches and complaints filed by employees, patients, and plan members through the OCR complaints portal. . Lack of Encryption or Alternative Safeguards While HIPAA does not demand the use of encryption, encryption is an addressable implementation specification and must be considered. The failure to use encryption or an alternative equivalent safeguard to ensure the confidentiality, integrity, and availability of ePHI has resulted in many healthcare data breaches. Security Awareness Training Failures HIPAA requires covered entities and business associates to implement a security awareness training program for all members of the workforce, including management. Training should be provided regularly and the frequency should be determined by means of a risk analysis. Improper Disposal of PHI When PHI or ePHI is no longer required it must be disposed of securely in a manner that ensures PHI is "unreadable, indecipherable, and otherwise cannot be reconstructed." Paper records should be shredded, burnt, pulped, or

pulverized, while electronic media should be cleared, purged, degaussed, or destroyed. Impermissible Disclosures of PHI An impermissible disclosure of PHI is a disclosure not permitted under the HIPAA Privacy Rule. This includes providing PHI to a third party without first obtaining consent from a patient and 'disclosures' when unencrypted portable electronic devices containing ePHI are stolen.

Electronically stored health information is now better secured than paper records ever were, and healthcare groups that have put in place mechanisms to adhere with HIPAA regulations are witnessing greater efficiency

Explaining HIPAA to Patients Healthcare organizations are now required by law to give patients a notice of their privacy practices and get patients to sign to confirm receipt of the document. A good practice to adopt is to put all relevant information in the Notice of Privacy Practices and then give patients a summary of what the policy contains. For instance, explain to the patient: ♣ They may request their medical records whenever they like. ♣ They may request you amend their medical records to correct errors. ♣ They can limit who has access to their personal health information. ♣ They can choose how you communicate with them. ♣ They have right to complain about the unauthorized disclosure of their PHI and suspected HIPAA violations. Healthcare Organizations and the Implications of HIPAA If data privacy and security is not adequately managed, the Office for Civil Rights can issue fines for non-compliance.