The Introduction of the Enforcement Rule

HIPAA History

Posted By Steve Alder on Dec 31, 2023

HIPAA History: Why was HIPAA Created?

Our HIPAA history lesson starts on August 21, 1996, when the Healthcare Insurance Portability and Accountability Act (HIPAA) was signed into law. HIPAA was created to "improve the portability and accountability of health insurance coverage" and the Act introduced a number of measures to ensure the continuity of coverage between jobs, guarantee coverage for employees with pre-existing conditions, and prevent "job lock" – a scenario in which plan members stayed in a job to avoid losing health benefits.

However, the measures introduced in the Act significantly increased costs for health insurers. To prevent the increased costs from being passed onto plan members and employers in the form of higher premiums, deductibles, and co-pays, Congress enacted further measures to combat waste, fraud, and abuse in health insurance and healthcare delivery, and to simplify the administration of health insurance transactions such as eligibility checks, authorizations, remittances, and payments.

As an increasing number of health insurance transactions were being conducted electronically, the Secretary for Health and Human Services (HHS) was instructed to develop standards to safeguard health information when it was maintained or transmitted electronically. The Secretary was also instructed to recommend standards for the privacy of individually identifiable health information. These instructions resulted in the HIPAA compliance guidelines of the Security and Privacy Rules.

The HIPAA Privacy and Security Rules Take Shape

Once HIPAA had been signed into law, the US Department of Health and Human Services set about creating the first HIPAA Privacy and Security Rules. The first "proposed" Privacy Rule was published in November 1999; but, due to the volume of comments from stakeholders, the "final" Privacy Rule was not published until August 2002. The Privacy Rule defines Protected Health Information (PHI), stipulates permissible uses and disclosures, lists the circumstances in which an authorization is required, and gives individuals rights over their PHI. The Privacy Rule had an effective compliance date of April 14, 2003.

The Security Rule took even longer to progress from "proposed" to "final". First "proposed" in August 1998, it was not until February 2003 that the "final" Rule was published; and, due to the number of implementation specifications, organizations were given longer to comply with the standards – the effective date of the Security Rule being April 21, 2005. Dealing with the subset of PHI that is created, collected, used, maintained, or transmitted electronically (ePHI), the Security Rule includes three sets of safeguards that must be complied with by covered entities and business associates:

- **Administrative** – covering topics such as risk analyses, workforce clearance, security training, access management, and contingency planning.

Exhibit 2005
Datavant v. Vigilytics
IPR2024-00307

- **Physical** – covering topics such as physical access to devices maintaining ePHI, device security, data back-ups, and the secure disposal of data and devices.
- **Technical** – covering topics such as password management, automatic logoff, data encryption, audit controls, and transmission security.

When Did HIPAA go into Effect?

The HIPAA effective date varies by provision. Many of the provisions in Title I – the title relating to the portability and accountability of health insurance coverage – went into effect within a year, while some of the tax-related provisions in Titles III and V were effective immediately.

The first two "Administrative Simplification Rules" – the HIPAA Privacy and Security Rules – evolved from Title II of HIPAA, and each had a different HIPAA effective date depending on the size and nature of the organization. For example:

- The HIPAA Privacy Rule became effective in April 2003 for most organizations. However, small health plans were given an extension of one year and the HIPAA Privacy Rule became effective for small health plans in April 2004.
- The HIPAA Security Rule became effective in April 2005 for most organizations. However, small health plans were again given an extension of one year and the HIPAA Security Rule became effective for small health plans in April 2006.

The Breach Notification Rule became effective in September 23, 2009, regardless of the size or nature of the organization, and there was no distinction between compliance capabilities in March 2013 when the Final Omnibus Rule made changes to the Privacy and Security Rules as required by the HITECH Act – although covered entities and business associates were not required to comply until September 2013.

Although the Department of Health and Human Services already had the authority to investigate complaints against covered entities for failing to comply with the Privacy Rule, the Enforcement Rule of March 2006 explained how the agency would conduct investigations and issue civil monetary penalties if a suitable resolution could not be achieved by voluntary compliance.

The Enforcement Rule also expanded the compliance and investigation provisions to all of the HIPAA Rules, rather than just the Privacy Rule. The authority to investigate complaints related to the Privacy and Security Rules (and later the Breach Notification Rule) was delegated to HHS´ Office for Civil Rights (OCR), while the authority to investigate complaints related to the Administrative Requirements (Part 162) was delegated to HHS´ Centers for Medicare and Medicaid Services (CMS).

HITECH 2009 and the Breach Notification Rule

HIPAA history continued in 2009 with the introduction of the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH had the primary goal of incentivizing healthcare providers to implement Electronic Health Records (EHRs) by introducing the Meaningful Use incentive program. Stage one of Meaningful Use was rolled out the following year and continued until 2018 when it was replaced with the Promoting Interoperability Program.

With the incentive program also came an extension of HIPAA Rules to business associates and third-party suppliers to covered entities, and the introduction of the Breach Notification Rule – a Rule that stipulated all breaches of PHI must be notified to affected individuals and to the Department of Health and Human Services' Office for Civil Rights. The criteria for reporting breaches of ePHI were subsequently extended in the Final Omnibus Rule of March 2013.

The Final Omnibus Rule of 2013

The most recent act of legislation in HIPAA history was the Final Omnibus Rule of 2013. The rule barely introduced any new legislation, but filled gaps in existing HIPAA standards – for example, specifying the encryption standards that need to be applied in order to render ePHI unusable, undecipherable, and unreadable in the event of a breach.

Many definitions were amended or added to clear up grey areas – for example, the definition of "workforce" was amended to make it clear that the term includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of the covered entity or business associate.

The Privacy and Security Rules were also amended to allow patient´s health information to be held indefinitely (the previous legislation had stipulated it be held for fifty years), while new procedures were written into the Breach Notification Rule. New penalties were also applied – as dictated by HITECH – to covered entities that fell afoul of the HIPAA Enforcement Rule.

HIPAA History Timeline

- August 1996 – HIPAA Signed into Law by President Bill Clinton.
- April 2003 – Effective Date of the HIPAA Privacy Rule.

- April 2005 – Effective Date of the HIPAA Security Rule.
- March 2006 – Effective Date of the HIPAA Breach Enforcement Rule.
- September 2009 – Effective date of the Breach Notification Rule.
- March 2013 – Effective Date of the Final Omnibus Rule.

In certain circumstances, covered entities and business associates were given an extended period of time to comply with the provisions of each Rule. For example, although the effective date of the Final Omnibus Rule was March 2013, covered entities and business associates were allowed 180 days to comply. Further key dates in HIPAA History can be found in our infographic below.

Consequences of the Final Omnibus Rule

What the Final Omnibus Rule achieved more than any previous legislation was to make covered entities and business associates more aware of the HIPAA safeguards they had to adhere to. Many healthcare organizations – who had been in breach of HIPAA for almost a decade – implemented a number of measures to comply with the regulations, such as using data encryption on portable devices and computer networks, implementing secure messaging solutions for internal communications with care teams, installing web filters, and taking more care to archive emails securely.

The financial penalties subsequently issued for data breaches – along with the colossal costs of issuing breach notifications, providing credit monitoring services, and conducting damage mitigation – make investment in new technology to protect data appear cheap by comparison.

10 HIPAA BREACH COSTS You Should Be Aware Of

"HIPAA Breaches Cost Approximately $200 Per Victim"

1

Breach Investigations

An external organization must investigate the breach to identify the cause and ensure that unauthorized access to PHI has been blocked.

2

Remediation

All of the safeguards which should have been installed to prevent a breach must now be implemented, under the close scrutiny of the Office for Civil Rights and the general public.

3

Temporary Operational Changes

A data breach places a considerable administrativeburden on healthcare providers. Staff must issue notifications, update websites, field customer queries, placate stakeholders and implement new safeguards. Healthcare services may be affected.

4

Breach Notification Letters

Breach notification letters must be issued to all affected individuals by first class post (49c). Subsequent notifications may need to be sent with updated information. One letter would cost Anthem 40M in postage costs alone.

5

Identify Theft Prevention

HIPAA requires covered entities to provide free credit monitoring and identity theft protection to all breach victims. The current cost is estimated to be $10 per individual, per month. Services must be offered for 1-2 years.

6

Regulatory Fines – Office for Civil Rights

The Office for Civil Rights issues financial penalties for HIPAA violations up to a maximum of $1.5 million per year, per violation category. The highest fine issued to date was $4.8 Million for a breach involving 6,800 individuals.

7

Regulatory Fines – Attorney General's Offices

Attorney Generals Offices assist the OCR in policing HIPAA Privacy and Security Rules. State AG offices are issuing fines for HIPAA breaches at a state level of up to $25,000 per violation category.

8

Lost Business / Loss of Reputation

Providers can expect a patient churn rate of 5-6% following a data breach, while 65% of consumers would consider switching providers after a major HIPAA data breach.

9

Class Action Lawsuits

Anthem had three class action lawsuits filed in the first 24 hours after the breach. Class action lawsuits usually claim damages of $1,000 per victim. Negligence claims may also be filed against healthcare providers for exposing PHI.

10

Website/Helpline For Breach Victims

HIPAA requires covered-entities to publish information on a company – or dedicated - website as well as provide victims with a free telephone number to allow them to obtain further information.

© Copyright 2024. All rights reserved.

The HIPAA Compliance Audit Program

In 2011, HHS' Office for Civil Rights (OCR) commenced a series of pilot HIPAA compliance audits to assess how well healthcare providers were implementing HIPAA Privacy and Security Rules. The first round of audits was completed in 2012 and highlighted the dire state of compliance.

Audited organizations registered numerous violations of the HIPAA Breach Notification Rule, Privacy Rule, and Security Rule, with the latter resulting in the highest number of violations. OCR issued action plans to help those organizations achieve compliance; however, for the second round of audits, it is not expected to be as lenient.

Audits are expected to target the specific areas that proved problematic for so many healthcare providers, while a permanent audit plan is being planned to ensure continued HIPAA compliance. The age of lax security standards has now passed and the healthcare industry, like the financial industry before it, must raise standards to ensure confidential data remains private.

Any covered entity that does not implement the required controls faces financial penalties, sanctions, potential loss of Medicare eligibility, and even criminal proceedings for failing to secure PHI.

How to Achieve HIPAA Compliance

Our "HIPAA Compliance Checklist" covers the elements of the Health Insurance Portability and Accountability Act relating to the storage, transmission, and disposal of electronic Protected Health Information, the actions organizations must take in response to a breach, and the policies and procedures which must be adopted to achieve compliance.

HIPAA regulations may be strict, yet covered organizations are allowed some flexibility on the privacy and security safeguards used to protect data. Data encryption, for instance, must be addressed but not necessarily implemented if other controls provide the necessary protection.

Some of the main technical safeguards used to protect and control ePHI actually help to streamline communication and information flow, and organizations that have adopted secure communications channels and implemented data controls have benefited from improved efficiency, faster response times, and improved patient outcomes, while ensuring that patient health data remains fully protected at all times.

More technical safeguards to secure ePHI and personal identifiers are no doubt in the planning stage now and will impact HIPAA history in the future. In the meantime, here is a brief HIPAA history timeline.

Milestones of the Health Insurance Portability and Accountability Act.

The Health Insurance Portability and Accountability Act of 1996 was introduced to improve coverage for workers changing employment and to raise standards of electronic healthcare transactions. The Act has been instrumental in ensuring the privacy of Americans is better protected.

There have been numerous updates to the legislation over the years to further improve healthcare data security and increase patient privacy rights.

This Infographic shows the key milestones in the 28-year history of The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct.

February 8, 2024

HHS Aligns SUD Protections Closer to HIPAA

The changes to 42 CFR Part 2 are intended to support the flow of information in organizations that participate in federally assisted Part 2 programs or that qualify as Part 2 service organizations.

The closer alignment of SUD records with HIPAA requires affected organizations to make changes to their HIPAA Notice of Privacy Practices, authorization procedures, and complaint handling processes.

October 5, 2023

Largest Attorney General HIPAA Settlement

A multistate action against a business associate resulted in a $49.5 million settlement and an extensive corrective action plan.

The attorneys general found the provider of donor relationship management software had failed to comply with the Security Rule and Breach Notification Rule following a ransomware attack in 2020.

February 2, 2023

FTC Issues First Penalty or Breach Notification Failures

In 2021, the FTC announced its intention to start actively enforcing the Health Breach Notification Rule which requires vendors of personal health records to notify consumers of unauthorized disclosures.

The FTC fined GoodRx Holdings $200,000

December 1, 2022

HHS Issues Guidance Regarding Online Tracking Technologies

The guidance related to the impermissible use of third-party tracking technologies on public-facing websites that could disclose PHI to third parties such as Facebook and Google.

for sharing health information with third parties such as Facebook, Google, and Twilio or advertising purposes without consent from consumers.

The guidance resulted in dozens of covered entities notifying HHS of data breaches attributable to the use of these technologies, and multiple lawsuits against healthcare providers alleged to have violated consumer protection laws.

March 20, 2020

First Notification of COVID-Era Enforcement Discretion

During the COVID pandemic, OCR announced four notifications of enforcement discretion to help support healthcare providers and business associates during the pandemic.

The notifications related to the provision of telehealth, public health oversight activities, community-based testing sites, and online scheduling apps, and remained in force until May 2023.

September 9, 2019

OCR Settles First Case in Right of Access Initiative

OCR's Right of Access initiative focused on healthcare providers that fail to respond to patient access requests within a timely manner.

The initiative resulted in forty-six settlements for HIPAA Right of Access failures between 2019 and 2023.

Ocobre 2018

Largest Ever HIPAA Penalty Issued

OCR has announced a settlement has been agreed with Anthem Inc., to resolve potential.

HIPAA Violations discovered during the investigation of its 78.8 million record data breach in 2015.

Anthem Inc., has paid OCR $16 million to settle the case.

April 2017

First HIPAA Settlement with a Wireless Health Provider

OCR announces its first ever HIPAA violation settlement with a wireless healthcare provider.

Cardionet agrees to settle the case with OCR for $2.5 million to resolve potential non-compliance with HIPAA Rules.

April 2017

First HIPAA Settlement for Phishing Attack

OCR has announced a settlement with a HIPAA-covered entity over a phishing attack.

February 2017

OCR Delays 2nd Phase On-Site Compliance Audits

OCR completes the 'desk audit' stage of

The attack potentially could have been prevented had HIPAA Rules have been followed. Metro Community Provider Network agrees to pay OCR $400,000 to settle the case.

January 2017

First Settlement for Tardy Breach Notifications

For the first time, OCR has settled a case with a HIPAA-covered entity solely for Breach Notification Rule violations.

Presence Health settled the case for $475,000 after unnecessarily delaying breach notifications.

December 2016

21st Century Cures Act Amends the HIPAA Privacy Rule

The 21st Century Cures Act is passed by the Senate.

The Act allows HIPAA-covered entities to disclose PHI for research related to the quality, safety, or effectiveness of a product or activity regulated by the FDA, updating the HIPAA Privacy Rule.

July 2016

OCR Confirms Ransomware Attacks Are Reportable Breaches

After a spate of ransomware attacks, OCR has confirmed that in most cases, ransomware attacks are reportable HIPAA breaches

Guidance on HIPAA and ransomware

the 2nd phase of HIPAA compliance audits on HIPAA-covered entities and business associates, but delays the onsite audits until 2018.

December 2016

HIPAA Enforcement Stepped Up

OCR has stepped up enforcement of HIPAA Rules, finishing the year with 12 settlements and one civil monetary penalty to settle violations of HIPAA Rules.

July 2016

First HIPAA Settlement for a Business Associate

OCR has announced the first HIPAA settlement with a business associate for the failure to comply with HIPAA Rules.

Catholic Health Care Services of the Archdiocese of Philadelphia agrees to pay $650,000 to settle the case.

March 2016

OCR Launches Second Phase of the HIPAA Compliance Audits

OCR confirms the much delayed second phase of its HIPAA compliance audit program has commenced.

HIPAA-covered entities and their business associates will be audited

attacks are released.

business associates will be audited.

The audits will guide future guidance and compliance tools.

November 2015

DOJ to Pursue Criminal Charges for HIPAA Violations

The Department of Justice announces a settlement with Warner Chilcott over criminal HIPAA violations.

DOJ explains it will aggressively pursue criminal charges against company employees and physician practice owners for HIPAA violations.

February 2015

OCR Confirms Start Date for the Phase 2 HIPAA Compliance Audits

OCR confirms the much delayed second phase of its compliance audit program will commence in 2016.

The delays have been due to pressure on OCR resources.

February 2015

OCR Updates HIPAA Breach Web Portal

OCR has completed the upgrade of its web portal, which now includes a 'wizard' to guide HIPAA-covered entities and their business associates through the breach reporting process.

Data breaches now need to be reported in greater detail to aid OCR's data breach investigations.

September 9, 2014

HIPAA Audits Delayed

OCR announces the second phase of the HIPAA compliance audits will be delayed, OCR requires additional time to implement and test its new data breach reporting portal.

The new web portal will be used by HIPAA-covered entities to report data breaches and will make it easier for OCR to collate paperwork and investigate breaches.

September 23, 2013

Omnibus Rule Compliance Deadline

The Omnibus Final Rule becomes enforceable and all covered entities, which now include business associates and their contractors, must abide by the new rule or face a financial penalty of up to 1.5 million per violation.

July 7, 2013

Technical Corrections to the Omnibus Rule

The comment period allowed covered entities and the public to voice concerns about the new Omnibus Rule, and the DHHS decides to make minor corrections to improve workability of the bill

The Omnibus Rule, Security Rule and Privacy Rule are to be assessed in the second round of 400 HIPAA compliance audits scheduled for late 2014.

March 26, 2013

Omnibus Rule Comes into Force

The Omnibus Rule takes effect and all HIPAA-covered entities must now comply with the new legislation.

The healthcare industry is given six months to comply before the rule will be enforced.

The new legislation also updates breach notification rules and Business Associates can now be held liable for breaches and certain HIPAA violations.

December 2012

OCR Compliance Pilot Audits End

The first round of compliance audits comes to an end revealing the poor state of HIPAA compliance.

The healthcare industry has been low to introduce the new changes required by the Privacy and Security Rule.

November 9, 2011

OCR Begins HIPAA Compliance Audits

The OCR begins its pilot round of audits.

115 audits are to be conducted on

by improving flexibility and decreasing the burned on covered entities.

January 17, 2013

HIPAA Omnibus Final Rule Issued

The DHHS releases the Omnibus Final Rule which incorporates the changes to HIPAA demanded by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

The new rule makes sweeping changes to improve data security, further restrict access to PHI, prevent the use of PHI for marketing and the Enforcement Rule is also enhanced.

March 24, 2012

Omnibus Final Rule Finalised

The Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules are received for review by the Whitehouse Office of Management and Budget.

The long awaited changes include a number of provisions of HITECH and involve major updates to HIPAA.

July 6, 2010

First Attorney General HIPAA Fine Issued

The Connecticut Attorney General is the

healthcare organizations, healthcare clearinghouses and health plans to determine the state of HIPAA compliance.

first to take action against a healthcare provider for failing to comply with HIPAA Privacy and Security Rules.

Health Net Inc. is fined $250,000 for the loss of an unencrypted hard drive containing the PHI of 1.5 million Americans.

February 27, 2010

HITECH Enforcement Begins

HITECH becomes enforceable and the new financial penalties now apply.

The healthcare industry must comply with the new regulations or face stiff penalties.

The healthcare industry is given a warning that compliance will be robustly enforced.

January 16, 2009

First OCR Settlement for HIPAA Violations

The OCR starts getting tough on violators of the HIPAA Privacy and Security Rules.

It starts a new year of increased enforcement by issuing its first financial penalty.

CVS Pharmacy Inc is ordered to pay $2.25 Million for improperly dumping patient health records.

October 29, 2009

HITECH Act Enforcement Interim Rule Issued

The HITECH Enforcement interim rule is issued, which introduces a new tiered structure of financial penalties or HIPAA violations based on four categories of culpability.

The rule significantly increases the fines for violations which can be up to $1.5 million per violation.

August 24, 2009

Breach Notifications Interim Regulations Issued

The DHHS introduces new regulations covering data breaches as demanded by the HITECH Act.

The new rules require covered entities to report data breaches to the OCR and notify potential victims of incidents which expose their personal and health information.

Febrary 17, 2009

HITECH Act Signed

The Health Information Technology

2008

OCR Lack of Enforcement

for Economic and Clinical Health Act (HITECH) is introduced as part of The American Recovery and Reinvestment Act of 2009 (ARRA).

The new legislation introduces incentives to improve information technology infrastructure and to encourage the use of electronic health record (EHR) systems.

OCR Lack of Enforcement Criticised

The OCR is criticized for its apparent lack of enforcement of the HIPAA and the Privacy and Security Rules, having issued no fines to organizations since being tasked with policing HIPAA.

In spite of more than 33,000 complaints up until 2008, only 8,000 were investigated and no financial penalties were issued.

The DHHS urges the OCR to get tough on offenders.

March 16, 2006

Enforcement Rule Goes into Effect

The Enforcement Rule is now in effect, marking the start of a new phase in HIPAA compliance.

The OCR is expected to start issuing financial penalties for any covered entity that fails to implement the requirements of the HIPAA Privacy and Security Rules.

April 21, 2005

HIPAA Security Rule Compliance Deadline

All covered healthcare organizations must now comply with the new requirements of the Security Rule and implement greater controls to keep health records secure and confidential.

The OCR can now issue civil penalties for violations.

April 18, 2005

HIPAA Enforcement Rule Proposed Rule

The HIPAA Enforcement Rule is proposed which will pave the way for OCR investigations into HIPAA violations and the issuing of financial penalties for HIPAA violations.

A procedure for hearings is also introduced.

October 16, 2003

Transactions and Code Sets Rule Deadline

The deadline is reached for adopting new codes for transactions and electronic exchanges, including new diagnosis and procedure codes.

The change is intended to increase standards and improve efficiencies in the healthcare industry.

April 14, 2003

HIPAA Privacy Rule Compliance Deadline

The Privacy Rule comes into effect and requires all covered entities to allow patients access to their health information on request, while limits are placed on how, when and to whom health records can be disclosed.

March 27, 2002

Proposed Privacy Rule Modified

The DHHS makes changes to the proposed Privacy Rule to clarify its provisions and to ease the administrative burden on healthcare providers.

December 20, 2000

HIPAA Proposed Privacy Rule Issued

The Privacy Final Rule is issued, only to receive technical corrections the following day.

The corrections cover compliance dates and access to Protected Health Information by the clergy while The Office for Civil Rights is delegated the responsibility of policing HIPAA.

August 12, 1998

Security and Electronic

Febrary 20, 2003

HIPAA Security Standards Final Rule Issued

The HIPAA Security Standards Final Rule (Security Rule) is issued and demands that all covered entities use the appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and security of electronic Protected Health Information.

Febrary 28, 2001

HIPAA Stumbles

The Privacy Final Rule technical corrections came into force on February 26th.

However the new Bush administration reopened the comment period, delaying the introduction of the new legislation.

November 3, 1999

Privacy Rule Proposed

The Privacy Rule is proposed to improve privacy standards and to restrict the disclosure of Protected Health Information and personal identifiers to unauthorized individuals.

Patients will also be given better access to their health data.

August 21,1996

Signature Standards Rule (Security Rule) Proposed

New legislation is proposed to further improve security standards to better protect individual health information stored by health plans, healthcare clearinghouses and healthcare providers.

The legislation also covers the use of electronic signatures by HIPAA covered entities.

HIPAA Introduced

Congress passes the Health Insurance Portability and Accountability Act (HIPAA).

Bill Clinton adds his signature to the legislation and the process of modernizing information exchange in the healthcare industry begins.

The bill also ensures workers do not lose health insurance coverage when changing employment.

© Copyright 2024. All rights reserved.

THE HIPAA JOURNAL

HIPAA History FAQs

Who Created HIPAA?

There is some dispute about who created HIPAA. While many sources refer to the Act as the Kennedy-Kassebaum Act after Ted Kennedy and Nancy Kassebaum – the two leading sponsors of a proposed "Health Insurance Reform Act" (S.1028) – the bill passed by Congress was S.1028´s companion bill HR.3103, introduced into the House of Representatives by Bill Archer with the original title of the "Health Coverage Availability and Affordability Act".

Why was HIPAA created?

The HIPAA Act was created with the original intention of reforming the health insurance market. According to a report by the Senate Labor and Human Resources Committee, the health insurance market at the time provided too little protection for individuals and families with pre-existing health problems. Many small businesses also found it difficult to obtain health coverage for employees at a fair price, while other workers could not transfer health benefits when they changed jobs.

Why was the HIPAA law created with additional privacy provisions?

To understand why the HIPAA law was created with additional privacy provisions, you have to look at the reason why Title II was created. One of the issues that could have prevented the passage of HIPAA was the costs health insurance companies would incur. To sweeten the pill, a second Title was added with the intention of preventing healthcare fraud and abuse – estimated to be costing health insurance companies billions of dollars per year due to fraudulent healthcare providers.

Title II of HIPAA created a national health care fraud and abuse plan based on standards for the electronic transmission of certain health information. To ensure health information transmitted electronically remained secure, the Secretary of Health and Human Services was tasked with establishing security standards; and in order to determine what data was subject to the standards, additional privacy provisions were established in the form of the Privacy Rule.

When was HIPAA enacted?

HIPAA was enacted at different times because it had multiple objectives. Some provisions of HIPAA were enacted retrospectively (i.e., changes to the Employee Retirement Income Security Act), while others were enacted within 30 days of HIPAA being passed (i.e., changes to the Internal Revenue Code in respect of Medical Savings Accounts). The majority were enacted within a year.

However, the section of HIPAA that had the biggest impact on organizations in the healthcare and health insurance industries – the Administrative Simplification provisions – was a new addition to the Social Security Act and was enacted in stages. The first "Final" Privacy Rule was published in 2000 (with a modified version published in 2002), and the Security Rule was published in 2003.

Why did regulators add new standards after HIPAA´s initial implementation?

Regulators added new standards after HIPAA´s initial implementation because, when the original "Final" Privacy Rule was published in December 2000, it attracted complaints from stakeholders and the public about the complexity of the Rule. Concerned that misunderstandings and confusion could unintentionally restrict patients´ rights and the quality of care, the Department of Health and Human Services modified the requirements and issued a second Final Rule in 2002.

In the preamble to the second Final Rule, there are multiple explanations of why new standards have been added and existing standards modified or removed. The majority of the changes related to the Minimum Necessary Standard, obtaining patient consent, Notices of Privacy Practices, marketing health-promoting activities and disclosing limited data sets for research purposes.

What is the history behind HIPAA?

The history behind HIPAA goes back to the 1960s when President Lyndon B. Johnson signed legislation that led to the development of the Medicare and Medicaid programs. Ever since, politicians have been trying to find ways to expand the Medicare program to all Americans. One of the leaders of the "Health Care for All" movement was Senator Ted Kennedy, who realized from his experiences in the 1970s and 1980s that "Small steps that address real needs and are politically palatable can be legislated more easily than wholesale reform."

When President Clinton´s 1992 election campaign pledges to reform healthcare and introduce a healthcare security card failed to get the support they needed, Senator Kennedy (with Senator Kassebaum) decided to take the "small step" of reforming the health insurance industry. In the end, their proposed "Health Insurance Reform Act" was rejected in favor of Representative Archer´s "Health Coverage Availability and Affordability Act" which evolved into HIPAA.

Why is the history of HIPAA important?

The history of HIPAA is important because it shows the progress of healthcare reform over the past sixty years. Much of the progress has been achieved in small steps, and in many cases, the progress has not kept pace with emerging technologies and threats to the privacy and security of health information. However, by looking back at what has been achieved in the past, legislators can be guided on how best to tackle future challenges.

Why was HIPAA enacted?

HIPAA was enacted primarily to reform the health insurance industry, reduce fraud and abuse by healthcare providers, and make the administration of claims processes more efficient. The HIPAA Privacy, Security, and Breach Notification Rules are effectively by-products of the primary objectives of HIPAA – even though they are now regarded as the "HIPAA Rules".

When did HIPAA start?

HIPAA started in 1996 when Congress passed the HIPAA Act. However, whereas most of HIPAA´s Title 1 provisions were enacted within a year of passage, the Administrative Simplification Regulations (the Rules many people regard as the HIPAA Rules) were not effective until many years later, starting in 2000 with the Standards for Electronic Transactions and Code Sets.

The Privacy Rule "started" being effective in 2003, and the Security Rule in 2005 – although neither was effectively enforced until after the publication of the Enforcement Rule in 2006. Later "start dates for HIPAA" occurred in 2009 with the Breach Notification Rule (which amended the burden of proof) and the Final Omnibus Rule of 2013 (which made Business Associates directly liable for data breaches).

When did the HIPAA Privacy Rule become effective?

The HIPAA Privacy Rule became effective on several dates. The first HIPAA Privacy Rule published in 2000 had an effective date of February 16, 2001. However, due to technical corrections, the effective date was initially delayed to April 14, 2001, before being further delayed to April 14, 2003, in order to address concerns over the complexity and workability of the Rule.

While most sources regard April 14, 2003, as the date when the HIPAA Privacy Rule became effective, at the time, the Rule only applied to Covered Entities. The effective date of the HIPAA Privacy Rule is later for Medicare Prescription Drug Card sponsors (January 1, 2006) and Business Associates of Covered Entities, who were not required to comply with the Privacy Rule ("where provided") until September 23, 2013 – the effective date of the Final Omnibus Rule.

HIPAA or HIPPA?

The acronym HIPAA is sometimes misspelled as HIPPA. HIPAA is the correct acronym to use as it stands for the Health Insurance Portability and Accountability Act. However, it is understandable the wrong acronym is sometimes used due to several widely

published authors referring to the Act in 2003 as the "Health Insurance Privacy and Portability Act" and the introduction of a bill into Congress in 2013 entitled the "Health Information Privacy Protection Act".

What circumstances brought about the HIPAA legislation?

The circumstances that brought about the HIPAA legislation were President Clinton´s election pledges in 1992. President Clinton had pledged to make Medicare available to all under a system similar to the UK´s National Health Service. However, once elected, President Clinton did not have the support to push his healthcare reforms through Congress.

The primary objective of HIPAA – to reform the health insurance industry – was a compromise solution championed by former "Health Care for All" advocate, Senator Ted Kennedy. Together with Senator Kassebaum, Senator Kennedy introduced the "Health Insurance Reform Act"; which, although rejected in favor of Representative Archer´s "Health Coverage Availability and Affordability Act", laid the foundations for the version of HIPAA that passed both houses in 1996.

In order for the health insurance industry to agree to the provisions of the Act without passing the cost of compliance onto plan members and employers, Congress added a second Title to the Act which included measures to reduce fraud against the health insurance industry and make the claims process more efficient. The standards subsequently published to make the claims process more efficient subsequently evolved into the Privacy, Security, and Breach Notification Rules.

Who created HIPAA?

Much of HIPAA was created by the Clinton Health Plan Task Force inasmuch as many of the measures that appeared in HIPAA were lifted from President Clinton's unsuccessful Health Plan and championed by legislators such as Senators Ted Kennedy and Nancy Kassebaum, who campaigned for several years to have their "Health Insurance Reform Act" passed in both houses. In the end, a companion bill introduced by Representative Bill Archer – the "Health Coverage Availability and Affordability Act" – was adopted by Congress. The name of the bill was amended to the Health Insurance Portability and Accountability Act as it passed through Congress.

Which stories rarely get told in the history of HIPAA?

The stories that rarely get told in the history of HIPAA relate to the compromises that had to be made to get the bill passed in both houses and the scale of healthcare fraud and abuse that the Department of Health and Human Services had to account for when developing the Administrative Simplification Requirements, the Privacy Rule, and the Security Rule.

With regards to the compromises that had to be made, provisions relating to insurance coverage for mental illnesses had to be dropped, as did most of the provisions intended to reform liability in medical malpractice cases. In addition, provisions allowing for medical savings accounts were added by the House of Representatives after the bill had passed the Senate.

The scale of healthcare fraud and abuse was never raised in the text of HIPAA. However, at the time it was estimated that healthcare spending in the US amounted to 1 trillion dollars, and that "as much as 10 percent of total healthcare costs are lost to fraudulent or abusive practices by unscrupulous healthcare providers" (Source: Report to House Ways and Means Committee, March 1996).

Has HIPAA been modified since it was enacted in 1996?

HIPAA has not been modified since it was enacted in 1996 because HIPAA is a federal law that amends or adds to existing US Code – for example the Internal Revenue Code via amendments to the Employee Retirement Income Security Act (ERISA) and the Public Health Service Code via amendments to the Social Security Act. Although ERISA and the Social Security Act have since been further amended, the amendments are not attributable to modifications to HIPAA.

It is also important to note that the Privacy, Security, and Breach Notification Rules that evolved from HIPAA are "regulations adopted by a federal agency" rather than a law passed by Congress. Although the Privacy, Security, and Enforcement Rules were modified by HITECH via the Final Omnibus Rule, the modifications were modifications to regulations rather than a modification to a law.

What differences to the history of HIPAA are attributable to the HITECH Act?

The differences to the history of HIPAA attributable to the HITECH Act are the Breach Notification Rule and the amendments to the Privacy, Security, and Enforcement Rules.

The Breach Notification Rule is not only significant because it required Covered Entities to notify individuals and HHS´ Office for Civil Rights of breaches of unsecured PHI, but also because previously HHS´ Office for Civil Rights had to demonstrate an individual had suffered harm before being able to pursue enforcement action. The Rule reversed the "burden of proof" so that Covered Entities had to prove a low probability of harm if not reporting a breach of unsecured PHI.

With regards to the amendments to the Privacy, Security, and Enforcement Rules, these can be summarized as follows:

- Business Associates were made directly liable for compliance with the Privacy, Security, and Breach Notification standards.
- The limitations on the use of PHI for marketing and fundraising were strengthened, as were the conditions for the sale of PHI.
- Individuals´ rights were expanded so they could receive electronic copies of PHI and restrict disclosures to health plans.
- Changes were required for Notices of Privacy Practices which had to be redistributed to patients and plan members.
- Authorization forms had to be modified to allow for disclosures relating to child immunizations, access to decedent information, and research.
- A new table of civil monetary penalties was introduced for violations of HIPAA attributable to willful neglect.

In what year was HIPAA signed into law?

HIPAA was signed into law on August 21, 1996. The important section of the Act for healthcare providers was Title II – which led to the publication of the Administrative Simplification Regulations. The HIPAA Administrative Simplifications Regulations include the Privacy Rule, the Security Rule, and the Breach Notification Rule.

How did HIPAA come about?

HIPAA came about due to a perceived need to reform the health insurance industry. Prior to 1996, some employees were locked into less-than-optimal jobs because changing employers would have meant the loss of health benefits. Other employees, who developed health conditions while employed by one employer, would have been excluded from health benefits by another employer.

Title I of HIPAA resolved the issue by requiring health plans to carry forward health benefits from one employer to another. But, because of the costs that would be incurred by the health plans – and the fear the costs would be passed onto employers and plan members as higher premiums – Congress passed Title II of HIPAA with the intention of combating fraud in the healthcare industry and simplifying the administration of health insurance transactions to save health plans money.

When did HIPAA become law?

HIPAA became law on August 21, 1996. Some Titles of HIPAA (i.e., Title III and Title V) became effective immediately, while most of Title I was effective within a year. Among other provisions, Title II – which contains the Administrative Simplification Requirements – instructed the Secretary for Health & Human Services to develop standards for the privacy and security of health information. These standards became effective in April 2003 and April 2005 respectively.

Why was HIPAA initially established?

HIPAA was initially established to reform the health insurance industry. Due to the way previous health insurance Acts were applied (i.e., ERISA and COBRA), some employees found themselves stuck in a “job lock” situation in which they could not change jobs because they would have lost their health benefits. The establishment of HIPAA changed this by enforcing the portability of health insurance between jobs.

“Healthcare HIPAA” (i.e., the Privacy and Security Rules”) was established due to concerns that the enforcement of health insurance portability would lead to higher costs for the health insurance industry, and that the costs would be passed onto employers and plan members as higher premiums. “Healthcare HIPAA” was one of a series of measures introduced in Title II of HIPAA to combat waste and fraud, and simplify the administration of health insurance transactions.

What changes to HIPAA since 1996 have there been?

There have been hundreds of changes to HIPAA since 1996 due to HIPAA amending multiple sections of Acts such as the Public Health Service Act, the Social Security Act, and the Employee Retirement Income Security Act. There have also been many changes to the HIPAA Administrative Simplification Regulations (“Healthcare HIPAA”) due to the frequency with which transaction codes in Part 162 of HIPAA are added and amended.

When was HIPAA established?

The answer to when was HIPAA established depends on which areas of HIPAA you are referring to. Some tax-related areas of Titles III and V were established immediately, while most health insurance-related areas of Title I were established within a year of the Act’s passage. Areas of HIPAA among the longest to establish include the Privacy and Security Rules of the HIPAA Administrative Simplification Regulations (part of Title II), which were not effective until April 2003 and April 2005 respectively.

What Rules were added to HIPAA in 2013?

There were no new Rules added to HIPAA in 2013. The Omnibus HIPAA Final Rule of 2013 amended the existing Privacy, Security, and Breach Notification Rules to account for changes required by the HITECH Act and GINA Act, and to address issues that had been identified in the three existing Rules to "improve their workability and effectiveness and to increase flexibility for and decrease the burden on the regulated entities".

How long has HIPAA been around?

HIPAA has been around – as the Health Insurance Portability and Accountability Act – since 1996. However, many of its provisions amended existing laws. As some of the laws amended by HIPAA are part of the Internal Revenue Code created by the Employee Retirement Income Security Act of 1974, it could be argued that HIPAA has been around far longer than many people imagine.

When was HIPAA passed?

HIPAA was passed in its original form (HR.3103) by the House on March 28, 1996, and in the Senate on April 23, 1996, in lieu of S.1028 (the "Kennedy-Kassebaum Act"). The Act subsequently went through two committee conferences in July 1996 with the committee reports being agreed by both chambers of Congress in August 1996. The Act was presented to President Clinton on August 9, 1996, and was signed into law on August 21, 1996.