Accedere

SOC 2 for HIPAA Compliance

Table of Contents

HIPAA Privacy Compliance

The HIPAA Act was effective in 1996, the HITECH Act in 2009 and the Final Omnibus Rule in 2013 and despite years passed by, HIPAA Privacy compliance is still a challenge for many health care organizations. We have several breach incidents relating to PII and specifically PHI. Organizations are still facing challenge in compliance and most findings relate to basic security hygiene such as risk management, policies, data minimization and encryption. Organizations are being fined in millions and their names appear in the Wall of Shame by HHS.

Once such 2019 case study is described below which relates to unencrypted data in a flash drive.

2019 HIPAA Case Study- University of Rochester Medical Center (URMC)

Incident & Fine

Data Theft: Unencrypted flash drive lost, containing ePHI. A $ 3 million fine was levied.

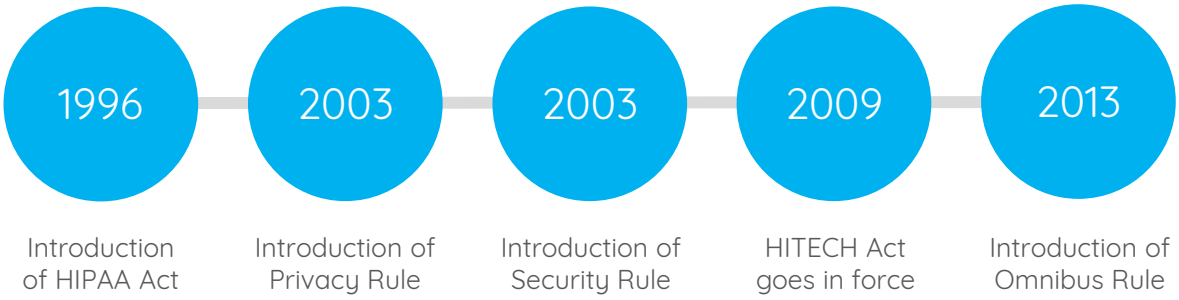
Findings

UMRC failed to conduct an accurate and thorough risk analysis, and implement policies, procedures, encryption mechanisms to encrypt/decrypt ePHI and security measures to reduce risks.

Compliance Agreement

Corrective action plan to include risk analysis, risk management plan; review and revise policies & procedures and evaluate any environmental changes.

The HIPAA Journey



The HIPAA compliance journey started in 1996, and the Privacy and Security Rules in 2003. The HITECH Act came into force in 2009 and clarifications via a final Omnibus Rule in 2013.

Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

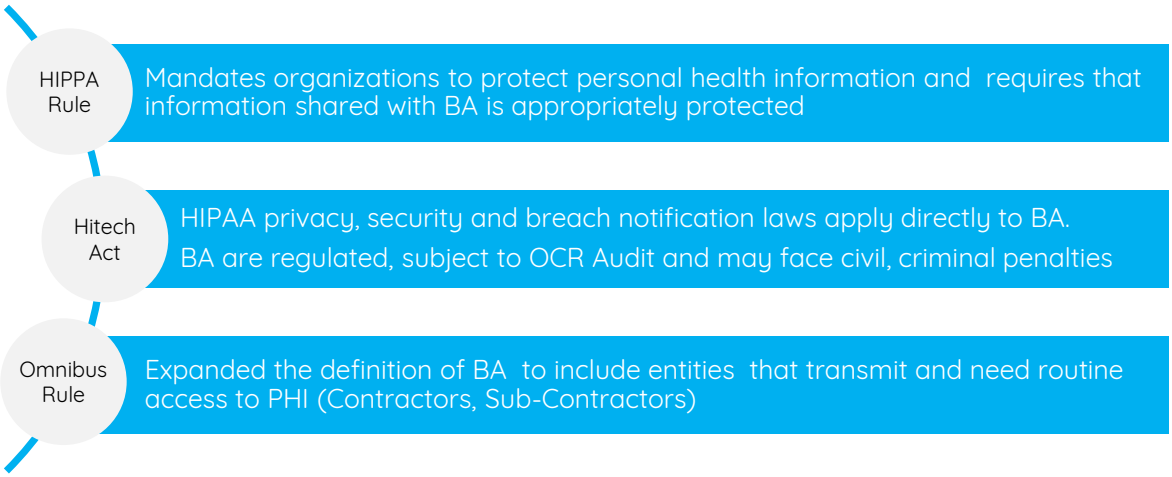
HITECH Act

The HITECH Act requires entities covered by the HIPAA to report data breaches, which affect 500 or more persons, to the United States Department of Health and Human Services (U.S.HHS), to the news media, and to the people affected by the data breaches. This subtitle extends the complete Privacy and Security Provisions of HIPAA to the business associates of covered entities. This includes the extension of updated civil and criminal penalties to the pertinent business associates. These changes are also required to be included in any business-associate agreements among the covered entities.

Omnibus Rule

covering Breach Notification and Enforcement Rules

In January 2013, HIPAA was updated via the Final Omnibus Rule. The updates included changes to the Security Rule, Breach Notification Rule and Enforcement Rule as required under the HITECH Act. The most significant changes were related to business associates directly responsible for compliance and prohibiting the sale of protected health information without individual authorization.



HIPAA Cyber Challenges

New technologies are evolving, and the health care industry has moved away from paper processes and now relies heavily on the use of electronic information systems to store and process the data. The cloud movement has an impact on healthcare industry too as majority of organizations have move to the cloud for its various benefits.

Today, healthcare providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems majority hosted in some sort of cloud environment.

The cloud environment is not safe either. One of the top cloud risks is the misconfigured servers that can lead to data breaches. Another major risk is insecure API's. Organizations use API's to transfer data to the business partners without a secure architecture in place and without conducting a proper vendor due diligence and evaluating the data flow lifecycle risks.

As required under the HIPAA rules the healthcare organizations are required to have a Business Associate Agreement with their vendors or the third-parties. It is equally important to understand the data security controls with their business associates.

Top Cloud Challenges

Rising Cyber Attacks in Healthcare

Number of records breached in 2019 were 27.5M up by almost 240%

Total number of Health care breaches in 2019 were 386 up by 33%

Total approximate cost of 2019 health care breaches was $11.8Billon

In 2019, Hacking and IT Incidents led to 60.6% of healthcare breaches

Source Bitglass Healthcare Breach report 2020

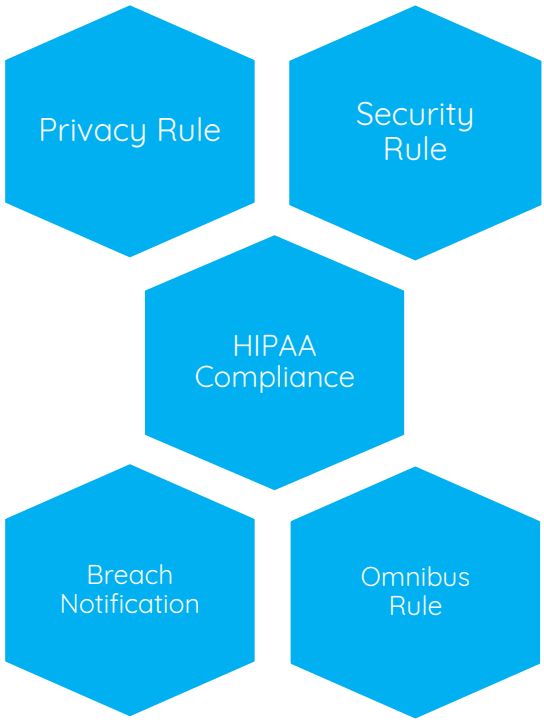
Why Healthcare Data is Lucrative

- Healthcare service providers have huge databases with more extensive customer information than any other industry.
- Health information sold for approximately $ 2000, much more than credit card or any other data.
- Medical identity theft is often not immediately identified by a patient or their provider giving a fraudster enough time to milk the credentials.
- Sensitive data easily accessible through connected devices.
- Low security controls across the industry makes it easy for hackers to get large amount of personal data.

HIPAA Compliance Requirements

Health care entities and related business associates (BA e.g., health plans, health care clearinghouses, exchanges, health care providers, and organizations that conduct certain financial, research, and administrative functions) are being asked with increased frequency to demonstrate that they meet the common security and privacy requirements of HIPAA that they have taken appropriate measures to:

- Secure their environment.
- Be vigilant in anticipating what might occur in the evolving security landscape.
- Implement appropriate measures to detect and react to existing and emerging threats.
- Be resilient in their ability to recover operations when a security incident does occur.
- Use encryption technologies to de-identity PII data.



Non-Compliance Implications

Organizations that fail to properly implement required controls or safeguards to protect PHI may experience severe financial penalties, the imposition of corrective action plans, or ongoing oversight by regulators over a multi-year period. Other risks include the adverse publicity of breaches and damage to their brand.

Assurance for HIPAA Compliance

The SOC 2 compliance report provides an assurance to the internal and external stakeholders of the organization, the specific controls implemented and/or operating effectively for complying with privacy regulatory requirements. A single SOC 2 report can provide information about the organization's controls over protected health information (PHI) based on the AICPA's Privacy Trust Services Criteria and HIPAA requirements. This SOC 2 examination can provide service organizations with the ability to increase transparency and communicate through a single deliverable to customers, business partners, and stakeholders both in and outside the healthcare sector. Healthcare covered entities should also demand a SOC 2 report from their business associates, CSP's to understand and to have an assurance over the controls implemented and/or operating effectives of the controls at the business associate or CSP over PHI Data Security as well as Privacy.

SOC 2 for Privacy and HIPAA

SOC 2 uses the AICPA Trust Services Criteria (TSC) for Privacy .With approximately 50 points of focus, the TSC organizes the privacy criteria as:

- Notice and communication of objectives—The entity provides notice to data subjects about its objectives related to privacy.
- Choice and consent—The entity communicates choices available regarding the collection, use, retention, disclosure and disposal of personal information to data subjects.
- Collection—The entity collects personal information to meet its objectives related to privacy.
- Use, retention and disposal—The entity limits the use, retention and disposal of personal information to meet its objectives related to privacy.

- Access—The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

- Disclosure and notification—The entity discloses personal information, with the consent of the subjects, to meet its objectives related to priv Notification of breaches and incidents is prov to affected data subjects, regulators and othe meet its objectives related to privacy.

- Quality—The entity collects and maintains accurate, up-to-date, complete and relevant personal information to meet its objectives re to privacy.

- Monitoring and enforcement—The entity mor compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints and disputes.

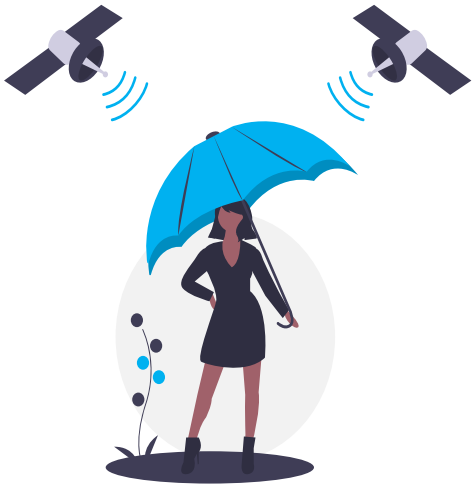
Aside from the Trust Services Criteria Privacy Controls, specific HIPAA requirements can also be covered.

SOC 2 for Privacy Benefits

- SOC 2 Type 2 can cover the entire year and the effectiveness of the controls in place.
- It is a Third-Party Period-of-Time assessment and so has Accountability.
- Most other assurance programs or audits are only, at a point in time.
- Since it is a period assessment, it is more like a continuous compliance with low risk and high reliability.
- Comprehensive Framework for Privacy by AICPA .
- Provides a high reliability SOC 2 Seal by AICPA.

We Can Help With Your HIPAA Compliance

We provide end to end SOC 2 examination report for HIPAA and Privacy compliance. We can cover all key requirements to provide and assurance of your compliance with the HIPAA requirements. In the SOC 2 compliance engagement for HIPAA we can additionally cover any specific privacy mandate to address your other compliance needs. Our unique delivery method improves timelines and thus reduces costs of your compliance. Our proven methodology saves times as well as costs thus giving you the benefit of timely compliance with reasonable costs.



Our Value Delivery

1. Experienced team in the area of Cyber Security.
2. Licensed CPA, Firm registered with PCAOB and Cloud Security Alliance.
3. Project management methodology applied to each engagement. These engagements are executed by senior professionals.
4. Prompt services with engagements completed in record time.
5. Ongoing support. We are with you whenever you need us.
6. Our services are competitively priced to provide you a higher ROI.