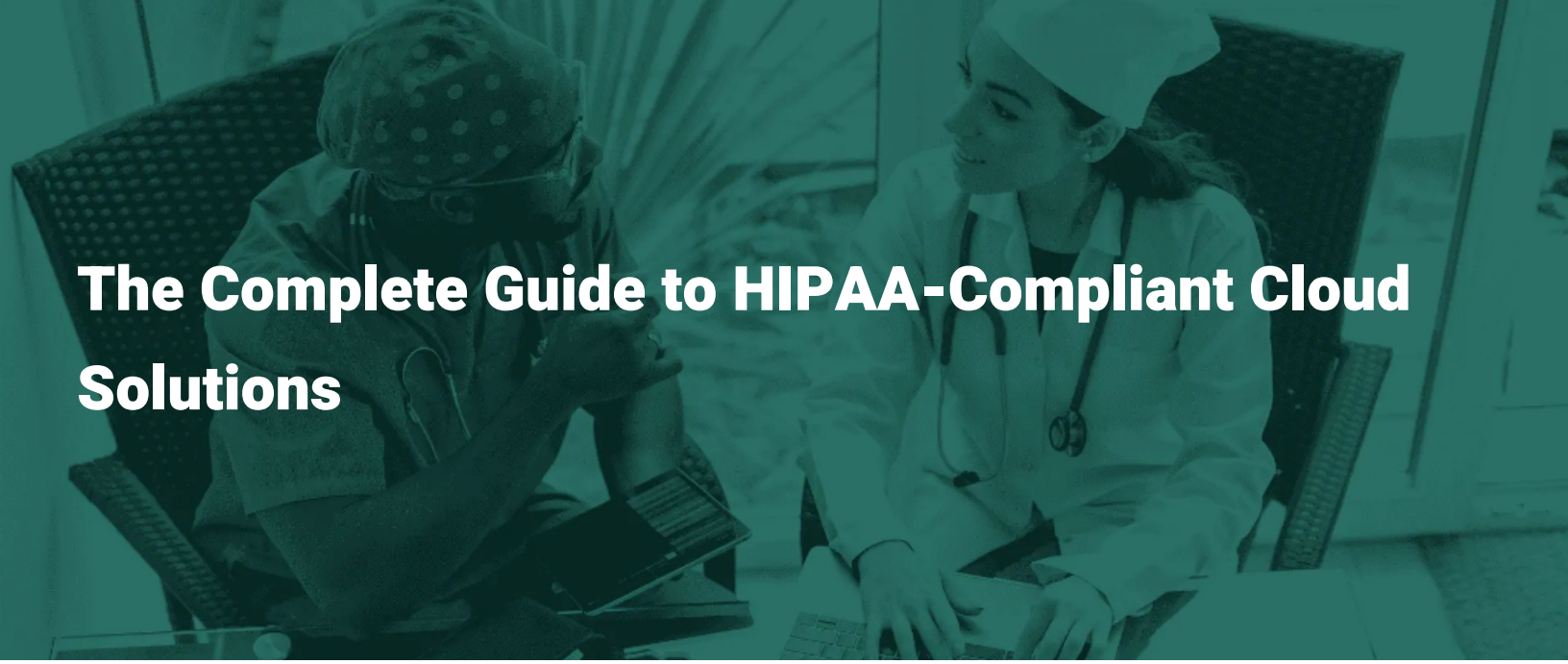


The Complete Guide to HIPAA-Compliant Cloud Solutions

The Complete Guide to HIPAA-Compliant Cloud Solutions

By Danijel Filipovic | White Paper | January 31, 2023

The Health Insurance Portability and Accountability Act (or HIPAA) of 1996 is the United State's premier federal regulation governing the storage, use, and transmission standards of personal health information (PHI) to protect patient privacy in accordance with the law.

Failure to comply with HIPAA exposes healthcare organizations to liability risk, reputational losses, and financial damage. As a healthcare service provider, it is essential to select technology vendors that deliver HIPAA-compliant software and services. Your organization needs to choose a software development partner that understands HIPAA and has completed information technology investment to deliver compliant software solutions that fulfill regulatory reporting and documentation requirements.

In 2022, more than 590 healthcare organizations experienced a data breach at an average cost of $4.35 million per event. HIPAA is the most significant piece of legislation governing patient privacy and the use, transmission, and storage of sensitive patient medical records. Failure to comply with HIPAA reporting standards exposes healthcare organizations to risk that is considered unacceptable by health insurance providers.

Healthcare organizations are being targeted by criminal organizations, criminal hacking syndicates, and state-backed hackers on a daily basis due to the immense value of personal health record (PHR) data on the dark web and other illicit marketplaces. In response, insurance providers are increasingly mandating third-party risk management encompassing implementing cybersecurity and data governance best practices.

In many cases, health organizations are unable to purchase insurance unless they can clearly demonstrate their organization's commitments to data security and ability to fulfill the reporting obligations of key pieces of legislation such as HIPAA.

The Three Pillars of HIPAA Compliance

Healthcare organizations and the third-party vendors they work with have a vested interest in delivering HIPAA-compliant software applications to reduce the opportunity for cybercriminals to access organizational data. The three pillars of HIPAA compliance were designed to protect patient privacy and limit the ability for personally identifiable personal health records to unlawfully enter the public domain.

In 2022, 12 data breaches were reported targeting healthcare organizations resulting in the loss of 1 million records, and a further 13 data breaches exposed between 500,000 and 1 million records. The vast majority of the losses were caused by supply chain cyber attacks against health insurance plans with additional attacks coming via business associates, healthcare clearinghouses, and providers.

HIPAA compliance is built on three pillars:

- **Confidentiality:** Personal health information must only be shared in approved methods with HIPPA-compliant entities
- **Integrity:** Data must remain preserved and unaltered whether intentionally or unintentionally
- **Access:** All stakeholders in the community healthcare matrix have proper and timely access to personal health records

Asahi Technologies delivers HIPAA-compliant healthcare software development services for enterprises. We build secure and reliable technology solutions to streamline the administrative burden caused by compliance obligations.

In this white paper, learn more about HIPAA-compliant cloud solutions.

What Are HIPAA-Compliant Cloud Computing Services?

Cloud-powered technology solutions are becoming popular all over the business landscape because of the scalability, cost-efficiency, and flexibility they deliver to healthcare organizations. Healthcare decision makers are adopting and implementing cloud services for the following reasons:

- **Expedited Deployment Times:** Cloud hosted services can be deployed instantly without the need for complex installation procedures. Deploy the services you need and implement healthcare technologies quicker using HIPAA-compliant cloud services.
- **Continuous Improvements:** Cloud services are updated continuously to ensure they are constantly improving. Leverage cloud solutions to deliver quicker product version that can be modified in real-time,
- **Secure Data Exchange Capabilities**: Enterprise cloud solutions deliver robust data exchange capabilities that ensure HIPAA compliance is a top of mind priority. Deliver data sharing across the healthcare matrix without compromising the integrity of private health data.
- **Reduced Costs:** Cloud solutions reduce the startup costs of purchasing new hardware and software.
- **Integrated Business Continuity Solutions:** HIPAA compliant cloud solutions already contain data security safeguards to protect sensitive organizational data.

May a HIPAA covered entity or business associate use a cloud service to store or process ePHI?

"Yes, provided the covered entity or business associate enters into a HIPAA-compliant business associate contract or agreement (BAA) with the CSP that will be creating, receiving, maintaining, or transmitting electronic protected health information (ePHI) on its behalf, and otherwise complies with the HIPAA Rules....

A covered entity (or business associate) that engages a CSP should understand the cloud computing environment or solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate BAAs." – **"Guidance on HIPAA & Cloud Computing" published by HHS.**

HIPAA-Compliant Cloud Storage Solutions are Essential for Healthcare Organizations

As far back as 2014, 90% of healthcare organizations had completed strategic investments in cloud storage solutions. Unfortunately in recent years, the healthcare industry has suffered an unprecedented crime wave which has placed providers on the front lines.

Nearly 80% of all healthcare data beaches in 2022 reported to the Health and Human Services' (HHS) Office of Civil Rights (OCR) were attributed to criminal hacking events, social engineering scams, and malware. Failure to safeguard patient health records exposes healthcare organizations to risk which threatens corporate risk management criteria.

Doctors, nurses, clinical experts, and medical researchers are all under specific obligations when it comes to recording, transmitting, retrieving, and sharing personal health information across the healthcare matrix. It is absolutely vital for healthcare information technology teams to spend considerable time and energy considering which technology solutions to allow their teams to use, limiting the use of software solutions like Zoom and Facebook Messenger which, though popular consumer-facing apps, do not offer HIPAA compliance.

The 5 Best HIPAA-Compliant Storage Solutions of 2023

Here are the 5 best HIPAA-compliant storage solutions of 2023. These cloud storage solutions are considered industry standards due to their reliance on implementing data security best practices to deliver HIPAA-compliant cloud computing. Use these cloud services to leverage solutions that offer the highest degrees of security, privacy and safety for healthcare service providers.

Google Cloud Drive

Since 2013, Google has been signing business associate agreements (BAA) to ensure HIPAA compliance across its GMAIL, Google Drive, Google Calendar, and G Suite services. Google Cloud Drive delivers HIPAA-compliant services backed by one of the world's largest development communities.

"G Suite incorporates all of the necessary controls to make it a HIPAA-compliant service and can therefore be used by HIPAA-covered entities to share PHI (in accordance with HIPAA Rules), provided the account is configured correctly and standard security practices are applied," explains the HIPAA Journal.

Microsoft OneDrive

Microsoft remains an industry leader for its commitments to the growth and proliferation of HIPAA-HITECH and has offered BAAs for its enterprise cloud services.

"Microsoft, when it provides services, including cloud services, to covered entities, enters into contracts to ensure that those business associates will adequately protect PHI. These contracts, or BAAs, clarify and limit how the business associate can handle PHI, and set forth each party's adherence to the security and privacy provisions set forth in HIPAA and the HITECH Act. Once a BAA is in place, Microsoft customers (covered entities) can use its services to process and store PHI," explains Microsoft.

Amazon (AWS)

Amazon S3 has emerged as one of the world's leading choices when it comes to HIPAA-compliant cloud computing services.

"In order to meet the HIPAA requirements applicable to our operating model, AWS aligns our HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule," states AWS on its compliance page.

Box

Box delivers comprehensive BAA support to ensure its products and services maintain HIPAA-HITECH compliance reporting standards.

"The Box platform and associated products have been compliant with HIPAA, HITECH, and the final HIPAA Omnibus rule since November 2012. All PHI stored in Box is secured in accordance with HIPAA, and Box signs BAAs with all clients who plan to store PHI in the cloud. Box continuously updates products, policies, and procedures to ensure continuous HIPAA compliance," according to Box for Healthcare.

Atlantic.Net

Atlantic.Net is one of the healthcare world's fully audited HIPAA and HITECH-compliant cloud service providers. This organization delivers comprehensive array of managed services that deliver cybersecurity, HIPAA-compliant hosting, and cloud storage requirements

What Are HIPAA-Compliant Digital Health Applications?

HIPAA compliance is a complex and nuanced requirement that mandates healthcare organizations to leverage information technology resources, cybersecurity strategies, and data management best practices as well as highlight the organizational professionals needed to execute and maintain them.

Building HIPAA-compliant software is essential for reducing risk and fulfilling corporate risk management criteria. Since the breakout of cyber crimes targeting healthcare organizations in recent years, insurance providers have placed a greater need for more robust security and data governance frameworks to limit the liability damage caused by cyber-attacks and data breaches.

It makes sense to develop customer-facing and provider-focused digital health solutions with compliance as a front-of-mind priority. As we move into the future, compliance obligations continue to climb and the fines associated with HIPAA violations increase.

To protect long-term profitability, healthcare organizations have a vested interest in releasing HIPAA-compliant software solutions to streamline administrative burden, reduce costs and protect institutional reputations.

YOUR GUIDE TO HIPAA compliant cloud solutions

Asahi TECHNOLOGIES

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a set of federal laws governing the storage, use, and transmission of personal health information to protect patients' privacy.

As a healthcare service provider, it is essential to select technology vendors that comply with HIPAA. Failure to do so exposes healthcare organizations to liability risk, reputational losses, and financial damage.

Cyberattacks on the rise

Vulnerabilities in the healthcare supply chain make health insurance plans easy prey for cybercrimes, with additional attacks coming via business associates, healthcare clearinghouses, and healthcare providers.

In 2022, the healthcare industry experienced:

12 data breaches

resulting in 1 million records lost.

And further

13 data breaches

exposing between 500 - 1 million more records.

The year set the highest record for data breaches since 2015 with 49.8 million.

Source: https://www.hipaajournal.com/editorial-lessons-from-biggest-hipaa-breaches-of-2022

Three pillars of HIPAA

Confidentiality

Personal health information must only be shared in approved methods with HIPAA-compliant entities.

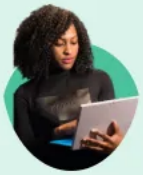
Integrity

Data must remain preserved and unaltered whether intentionally or unintentionally.

Access

All stakeholders in the community healthcare matrix have proper and timely access to personal health records.

HIPAA compliance checklist



- ☑ Regularly audit your cloud solutions to find and mitigate any system vulnerabilities
- ☑ Monitor and create detailed documentation of your software
- ☑ Provide proper training on privacy and security procedures to staff and business associates
- ☑ Develop and implement a robust remediation plan
- ☑ Promptly notify all relevant parties in the event of a breach

7 Key Questions to Ask Your HIPAA-Compliant Cloud Solutions Provider

Before your healthcare organization hires a cloud hosting provider, here are 7 key questions to ask to ensure they will deliver HIPAA compliant services:

What Are Your HIPAA-Compliant Hosting Services?

One of the most important questions to ask is what specific HIPAA-compliant measures your hosting provider has in place. Managed services are not a good fit for healthcare organizations due to the comprehensive HIPAA compliance reporting obligations.

What Evidence is There of Your HIPAA-Compliant Services?

Your hosting provider should be able to provide clear audit controls and compliance reports outlining their ability to fulfill all reporting requirements for HIPAA. If they can not provide evidence of HIPAA compliance, they may not be able to help protect your organization from liability damages.

Does Your Organization Offer BAAs?

BAAs are written agreements that address key privacy and liability concerns to protect healthcare organizations from data breaches and other violations of HIPAA.

What Steps Has Your Organization Taken to Audit its HIPAA Compliance?

There is no single standard to prove HIPAA compliance of software. However, your hosting provider should be able to provide audit report information covering SOC 1 Type II, HITRUST CSF, NIST, or SOC 2 Type II compliance measures. They should also be able to tell you what staff members are responsible for data collection and documentation processes.

Does Your Organization Have Incident Response Protocols?

An incident response plan describes how a CSP will respond to a data breach event and what steps will be taken to safeguard organizational data.

Has Your Organization Experienced a Data Breach?

It is very important to know if your provider has experienced data breaches in the past. Moreover, you will want to know what measures it has in place to protect your data against a breach in the future.

Who is Your Organization's Dedicated HIPAA Compliance Officer?

Covered entities and business associates are required to appoint a HIPAA compliance officer to oversee the implementation of privacy and security measures for PHI handled on the cloud.

Learn More About How Your Healthcare Organization Can Stay HIPAA-HITECH Compliant While Using Cloud Solutions

If you still have questions about the best cloud storage service providers and how to maintain solid HIPAA compliance, Asahi Technologies can help. Get in touch today to learn more about HIPAA-compliant cloud solutions.

Get in Touch