PLANET9

A Guide to HIPAA Security Compliance for Start-Ups

Content

Intro

Planet 9 Inc. is a California-based information security and compliance consulting company. Helping start-ups with HIPAA compliance and PHI security is the core of our business. Our professionals have experience working in different industries, including small businesses and large healthcare organizations.

Working in the healthcare industry for many years, we know how challenging it is for businesses to stay compliant with the Health Insurance Portability and Accountability Act (HIPAA) and meet the high bar set by customers. The biggest challenges are the lack of resources with security and compliance knowledge, along with the lack of awareness regarding the compliance requirements. In the early phases, companies hire essential staff to get the products and services to market. The staff typically includes healthcare professionals, data scientists, software developers, sales, etc. When the product or service is ready for market, the company starts talking to potential clients - usually larger companies with rigorous vendor security and compliance validation processes.

Since security and compliance are often considered non-essential during the early development phases, many start-ups have very little to show to their customers to demonstrate their adherence to compliance requirements and the security of their products. As a result, this creates significant delays for the start-ups in onboarding their customers. Since integrating security and compliance at the later development stages is always more expensive, companies end up spending more money and resources than they would've spent if they had integrated these requirements at the early stages.

This ebook provides start-ups with valuable information by clarifying some compliance mysteries and outlining clear steps for maintaining secure and compliant operations.

Start-up Compliance Misconceptions

The start-ups' HIPAA compliance and security approaches are full of misconceptions. Unfortunately, the decision-makers often make business decisions misled by wrong assumptions. When interacting with our clients, we hear many misconceptions from them. Some of the most common ones are:

01

"We use a cloud services provider (AWS, Azure, GCP, etc.), and they are responsible for our security and HIPAA Compliance."

Cloud service providers are typically responsible for the physical security of their data centers and the security of their cloud management platforms. Customers are accountable for other security and compliance processes, such as the security of hosts and databases, the development of secure applications, systems monitoring, and many other compliance aspects. Read more about how the shared responsibility model works in our blog: [Shared Responsibility Model: Addressing Key Challenges To Cloud Security.]()

Cloud services providers enable customers to build secure and compliant environments by providing various security solutions, but configuring and using these tools to get the security benefits they provide is the customers' obligation.

02

"We are too small to be targeted by cybercriminals."

Small businesses rarely become a prime target of cybercriminals. However, cyber-attacks are not necessarily targeted at a specific company; criminals run random opportunity scans to identify systems with vulnerabilities, and any vulnerable systems may be discovered with such scans.

Additionally, hackers do their homework. Was there a press release published about a start-up signing a contract with a big client? If so, that start-up is now on cybercriminals' target map. Hackers know that it is often much easier to get to their prime target through the target's vendors, who may have a lower cybersecurity posture. Read more about how small businesses provide criminals with initial access to large corporations in our blog posts: [Roadmap for Ransomware Protection]() and [2022 Cybersecurity Trends]().

Finally, many attacks come internally when unloyal employees exfiltrate, steal, or sell companies' secrets and other sensitive data. There are many cases when healthcare organizations report insider data breaches. Thus, internal threats should also be identified and assessed when designing your data security plan. More information about insider data incidents can be found in our article: Fall 2021: [Summary of Healthcare Data Breaches]().

03

“Our data is stored encrypted, so we are secure and compliant with HIPAA.”

Encryption is one of the key security technologies in reducing the risk of unauthorized data exposure. If the media where data is stored is stolen, encryption should prevent unauthorized access. At the same time, applications that use this data can access it in a decrypted format. Similarly, personnel working with the data need to have access to it. This means that if the application or database accounts are compromised, the perpetrators will access the data even when encrypted.

While encryption is a very effective security control, it is not a silver bullet. Data encryption is just one of many HIPAA Security Rule requirements, and it’s essential to address other threats to data security.

04

“Addressable standards provided in the HIPAA Security Rule are optional.”

There are required and addressable standards in the HIPAA Security Rule. However, it does not mean that addressable requirements are optional. In practice, the addressable standards must be analyzed for their applicability to the organization’s processes and technologies. Only when the analysis determines that they are not reasonable and appropriate, the organization may choose not to implement the standard and create a formal record of the analysis performed and decisions made.

What is HIPAA?

HIPAA is a US federal law adopted in 1996 to improve the efficiency and effectiveness of the national healthcare system. It requires covered entities and business associates to adopt national standards for electronic health care transactions as well as protects the privacy and security of Protected Health Information (PHI). Additionally, the law establishes breach notification requirements and penalties for noncompliance.

Under HIPAA, covered entities are individuals or organizations - doctors, clinics, hospitals, and insurance companies - providing healthcare services. Business associates are the covered entities’ vendors that store, process, or transmit PHI.

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) was adopted and further strengthened HIPAA by implementing steeper fines for noncompliance and stricter breach notification requirements. Also, business associates became directly accountable for complying with the regulation.

In 2013, the HIPAA Omnibus Final Rule was adopted. This regulation combined HIPAA and HITECH, provided further restrictions on the sale of PHI, and expanded patients' rights to access their data.

While HIPAA addresses many aspects of the healthcare system, we are focusing on the Security Rules.

The HIPAA Security Rule

The HIPAA Security Rule outlines requirements for protecting PHI that is created, received, maintained, or transmitted electronically (ePHI). A primary goal of the Security Rule is to sufficiently protect the individuals' health information while allowing businesses to conduct their operations and adopt new technologies. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

Specifically, the covered entities and business associates must: 1) ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; 2) identify and protect against reasonably anticipated threats to the security of ePHI; 3) protect against reasonably anticipated, impermissible uses or disclosures; and 4) ensure compliance by their workforce. To better understand the HIPAA Security Rule requirements, read the article [HIPAA Security Rule: Safeguards to Protect ePHI]() on our website.

The HIPAA Privacy Rule

The HIPAA Privacy Rule establishes requirements around legal uses and disclosures of PHI. The rule requires the implementation of appropriate safeguards to protect the privacy of PHI as well as gives individuals rights over their personal information. Such rights include examining their health records, obtaining copies, and requesting corrections. At the same time, the rule allows the secure healthcare data flow that is essential to promoting high-quality healthcare. In this way, the rule maintains the equilibrium that permits important uses of information while protecting the privacy of individuals. The basic principle of the Privacy Rule is limiting the circumstances in which the PHI may be used or disclosed by covered entities. Thus, the PHI may only be disclosed to: (1) individuals who are the subject of the information (or the individual's representative); (2) Health and Human Services (HHS) when it is undertaking a compliance investigation, review, or enforcement action; (3) carry out treatment, payment, and health care operations; (4) in case of Public Interest and Benefit Activities; etc. and (6) Limited Data Set for research, public health, or health care operations.

The Privacy Rule does not directly affect most start-ups unless they are covered entities. For business associates, the privacy of PHI is governed by Business Associate Agreement (BAA). BAA is a special agreement that spells out to business associates permissible data disclosures, breach notification timelines, and other requirements around PHI.

Privacy compliance is a different topic and not covered in this ebook.

Who Needs to Comply?

Virtually any business that stores, processes, transmits, or generates ePHI must comply with the HIPAA Security Rule. This statute includes covered entities and business associates. Acting mainly as business associates, healthcare start-ups are expected to be HIPAA compliant. BAA is signed when a covered entity engages a business associate to provide services in the scope of applicable operations involving PHI.

When a business associate signs BAA, they are legally bound to comply with HIPAA. It is important to note that many covered entities have a low-risk tolerance and require virtually all their vendors to sign BAAs even when accidental exposure of ePHI is possible. For example, instant messaging (IM) software may not be used by a covered entity to communicate ePHI. However, an employee may violate the policy and send PHI via IM. So when a product or service is not meant to be used for ePHI storage or transmission, HIPAA compliance should still be considered to ensure broader market adoption.

Why Comply?

There are many reasons why companies must comply with HIPAA, aside from the fact that protecting ePHI is a legal and moral obligation for all organizations. The pragmatic reasons for HIPAA compliance vary from assuring the safety and security of ePHI to avoiding steep fines for noncompliance. Specifically, the HIPAA compliance helps covered entities and business associates to:

01

Be a reliable business partner. Most covered entities have processes in place to assess their vendors' (business associates) compliance with HIPAA. If a vendor does not have sufficient policies, procedures, and technologies to protect

PHI, the covered entity will not sign the contract.

02

Assure safety and security of PHI. HIPAA compliance is a synonym of reliability in healthcare. In other words, by maintaining HIPAA compliance, covered entities and business associates can be more confident about safety and security of individuals' sensitive data they process.

03

Avoid fines. The Office of Civil Rights (OCR) conducts HIPAA audits of covered entities and business associates to ensure HIPAA compliance. When noncompliance or violation is found, the company may pay significant fines. In general, the fines for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation. Read our article HIPAA Compliance: Learning from the Others' Mistakes to learn more about the fines and other HIPAA enforcement actions.

04

Maintain reputation. If OCR auditors reveal any sign of HIPAA noncompliance during the HIPAA audit or a company experiences a data breach, this information becomes publicly available. Such situations do not reflect well on businesses and damages their public image. Thus, HIPAA compliance is one of the main prerequisites for maintaining the reputation of a reliable partner.

HIPAA compliance is vital for surviving in a healthcare environment, while noncompliance puts businesses at a strategic disadvantage and requires a longstanding recovery process. on-compliance may mean the end of the road for small businesses, as they won't be able to sustain damages, including fines and loss of customers.

How to Comply?

The first step in establishing a HIPAA compliance plan is conducting security risk and compliance assessments.

Security Risk Assessments
Compliance Assessments

It is important to clarify the difference between them. The HIPAA Security Rule provides a set of minimum requirements (safeguards) that organizations must implement to comply. A compliance assessment is an exercise of determining if the organization meets those minimum requirements. A security risk assessment, in contrast, is an exercise of determining and addressing threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The risk assessment aims to identify additional controls, above and beyond those provided in the HIPAA Security

Rule, necessary to effectively protect ePHI.

Conducting these two exercises will help the organization identify compliance gaps and security risks to ePHI and develop a plan for addressing them.

Compliance Assessment

The HIPAA Security Rule requires organizations to perform a periodic technical and non-technical assessment in response to environmental or operational changes affecting the security of ePHI. The assessment establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.

At the initial stage, the compliance assessment involves reviewing policies, procedures, and technological safeguards the organization already has to satisfy the HIPAA Security Rule requirements. Hence, by conducting a thorough review of operations and assessing areas responsible for maintaining the technical safeguards, organizations may evaluate their compliance and create a baseline for future evaluations. The article HIPAA Compliance Evaluation for Responding to Security-Related Challenges provides more in-depth information about compliance evaluations.

At the same time, the compliance assessment is a continuous process that aims to review any changes that may affect ePHI security. These may include any technical (hardware, software, media), environmental (physical location, facilities), or operational (people, processes) changes. These changes may occur when businesses decide to incorporate new technologies, move their assets to the cloud, or change hardware or software for a more sufficient one. Other factors that force the demand for compliance assessment include security incidents, new threats to ePHI security, changes to the organization's infrastructure, etc. A reassessment helps ensure that the organization's compliance status is intact when any of those changes occur.

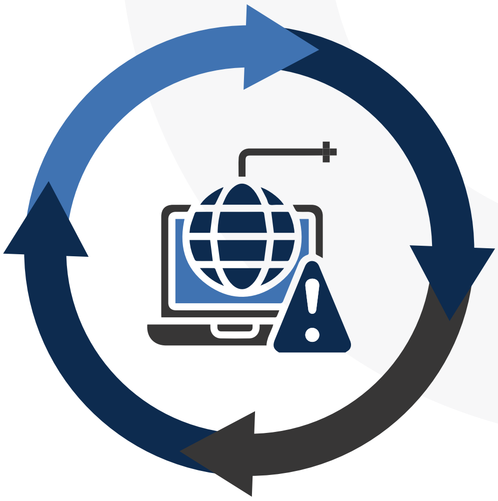
HIPAA Vitals

Compliance evaluation may be performed either internally or using external consultants. Without the experience, it is not easy to understand what exactly is necessary for HIPAA compliance just by reading the HIPAA Security Rule. To help organizations with their compliance evaluation efforts, Planet 9 developed the HIPAA Vitals application. HIPAA Vitals is a free tool that helps organizations conduct a thorough compliance self-assessment. The application provides HIPAA requirements and recommendations in plain English.

HIPAA Vitals

Risk Assessment

Not surprisingly, conducting thorough and accurate risk assessments is the first requirement under the HIPAA Security Rule. Risk assessment is a systematic process that addresses the undesirable adverse impacts to an organization's electronic and physical assets and provides a stable background for mitigating the identified risks. The risk assessment is essential for determining cybersecurity risk levels to which organizations may be exposed. It also gives a great opportunity to provide adequate actions and resources to treat those risks. Finally, it creates a risk awareness culture within the organization, so employees understand security risks and how these risks align with business objectives.



Risk assessment is a complex exercise that unites several important concepts and entails a series of necessary steps. A thorough risk assessment requires identifying the potential risks and vulnerabilities to the security of ePHI and gathering data on where the ePHI is stored. These steps help identify reasonably anticipated threats specific to the circumstances of the organization's environment and assess security measures that the organization already has. Based on this information, the organization can determine potential threats and vulnerabilities (risks) along with their probability and impact, followed by the development of a remediation plan to address those risks. A thorough description of the risk assessment process can be found in such reputable sources as ISO 27005, NIST SP 800-30.

Planet 9 published several articles to help organizations navigate through the risk management process: Answering Key Questions About Security Risk Assessments, How to Conduct a Risk Assessment? and Risk Assessment Under HIPAA Security Rule.

Key HIPAA Security Rule Requirements

Some of the most significant HIPAA Security Rule requirements also include the following:

01

Assigned Security Responsibility

It is critical to establish a formal role, such as Chief Information Security Officer (CISO), who is responsible for implementing HIPAA Security Rule requirements and managing the compliance program. The individual fulfilling the role must have sufficient knowledge and experience to manage the compliance program. Hiring a full-time CISO is a luxury that smaller businesses may not be able to afford. Small businesses and start-ups can benefit from using Virtual CISOs (vCISOs) that provide part-time or interim help in managing information security and compliance programs. Learn more about Virtual CISO services and get additional information about the vCISO solution for small businesses on our website.

02
Security Awareness and Training

HIPAA compliance requires a stable awareness culture within the organization for its employees to understand the importance of protecting the security of ePHI. For this purpose, organizations must establish a formal security awareness and training program and provide continuous education to all workforce members. Such training should address cybersecurity risks and best practices for working with ePHI in a compliant and secure manner. Providing periodic security reminders to all workforce members is also a good practice and part of the rule's requirements. Such reminders may be provided by sending periodic emails, posters placed throughout the office space, all-hands meetings, and other communication channels. Remember, humans are the weakest links in the security chain, and one person's mistake or negligence may cost the company significant financial losses and hinder their reputation.

03
Access Management

The Security Rule requires implementing policies and procedures for authorizing access to ePHI. Access to PHI must be provided only to those individuals who need to have access to it in order to do their job. All accesses to ePHI must be documented, periodically reviewed, and timely terminated when no longer required. Additionally, the individuals must be cleared by HR and receive appropriate training.

04
Events Logging and Monitoring

The HIPAA Security Rule obligates organizations to develop formal standards for logging systems activities related to ePHI access and processing. All system actions and respective outcomes must be logged. The logs must be securely stored and retained to support future investigations. It is also necessary to develop processes for monitoring those logs for suspicious activities related to ePHI access.

05
Data Storage and Transmission

ePHI data should be stored and transmitted in an encrypted format. Organizations must use secure encryption protocols for storing and transmitting ePHI. Per HHS guidance, valid encryption processes for data at rest are consistent with NIST Special Publications 800-111: Guide to Storage Encryption Technologies for End User Devices, 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77: Guide to IPsec VPNs; 800-113: Guide to SSL VPNs, or others that the Federal Information Processing

Standards (FIPS) 140-2 validated for data transmission.

06

Security Incident Management

Organizations must establish processes and procedures to address security incidents that may put ePHI's confidentiality, integrity, and availability at risk. A formal security incident response plan must be developed that identifies roles responsible for managing security incidents. It is also necessary to maintain a list of appropriate customer and authority contacts that may need to be notified. Finally, a breach notification procedure must be documented. Who to notify when a data breach event occurs? When to notify? What notification channels to use?

07

Business Continuity Planning

Organizations need to develop and test formal Business Continuity and Disaster Recovery Plans. The purpose of these plans is to ensure that there are people, processes, and technologies available to restore data and processes to the operational state in case of certain undesirable events (e.g., pandemia, natural disaster, system failure, data corruption, etc.). Our article Ensuring Business Continuity at the Time of Disaster provides additional information on this topic.

08

Third-Party Vendor Management

Organizations have to identify all third-party service providers that have or may have access to the ePHI they hold and ensure that a BAA is signed with each third party.

In addition, a process for managing third-party vendor risks must be in place. This may include conducting risk assessments of the third-party vendors or reviewing their independent audit reports and certifications, such as SOC 2 and HITRUST, on a periodic basis.

09

Physical Security

Maintaining physical security is also necessary when aiming for HIPAA compliance. It demands developing and implementing a physical security plan to address physical threats related to the company's offices and data centers where ePHI data is accessed and processed. Additionally, requirements must be developed for workstations used for ePHI data access on-premise and remotely.

10

Policies and Procedures

Organizations must develop formal information security policies and supporting documents that address all the requirements related to HIPAA compliance and ePHI data protection. It is also necessary to establish a process for reviewing and updating information security policies (at least annually), and when changes to business processes, technologies, regulations, and threat landscape occur. Each such document should have a change log to capture the following information: Who created the policy? Who approved the policy? When was it approved? When was it updated? What changes were made?

Establishing and Maintaining HIPAA Compliance Program

As previously mentioned, the state of compliance is a moving target. New business processes and technologies and adjustments to the existing ones, can change the state of compliance. For this reason, compliance has to be monitored and assessed on an ongoing basis. A successful compliance program should include the following elements:

Compliance Plan: The plan should be documented and should identify all the activities that need to be carried out as part of the compliance program. Examples of such processes and activities include compliance assessments, employee onboarding process, access reviews, compliance training, Business Continuity test exercises, technical compliance reviews, etc. Identify the frequency of these activities and assign individuals or teams responsible for them.

Ongoing Compliance Monitoring: Establish processes and methodologies for ongoing compliance monitoring. Are the required activities and processes executed as designed? Are they effective and efficient? This can be determined by using metrics and conducting internal and external audits.

Management Reporting: Create a process for reporting the status of your compliance program to the company's management. Establish a Security and Compliance Council group and include top management and representatives from all major business units. These meetings should be conducted on a periodic basis (monthly or quarterly). Risk assessment reports, audit reports, measurement metrics, incident reports, policy changes, and other relevant information should be reviewed in the scope of the council meetings.

Monitoring for Compliance Changes: Compliance requirements may change due to new regulations, customer contracts, business processes, and other factors. It is critical to review and update the compliance program when any changes occur. For example, your new customer is storing Medicare data, and now the service provider may need to comply with additional CMS requirements for entities participating in the Medicare program.

About Planet 9

Planet 9 provides compliance and security services to organizations across different industries, including healthcare, cybersecurity, cloud storage, digital advertisement, software development, revenue management, educational institutions, and others.

Our **mission** is to help businesses of any size and complexity to protect their sensitive data and comply with laws and regulations that address data security and privacy.

Our **core values** are outlined below:

- **Professionalism:** Conduct the work in a professional manner and take full accountability for it.
- **Transparency:** Ensure clients are always clear on what we are doing, how we are doing it, and why we are doing it.
- **Reliability:** Always deliver on our promises.

Why Planet 9?

We maintain a lean organizational structure that leverages the experience of seasoned security and compliance professionals. This model allows us to provide top-quality services at reasonable rates.

We also believe in forming long-term relationships with our clients to become their trusted advisors. We know each company is unique, so we do not use a cookie-cutter approach.

Instead, we take each client’s risk profile, financial capacities, and compliance requirements into consideration and recommend a unique solution that suits them.

About Planet 9

Main Services

Our main services include:

Information Security Services

Our vCISOs help clients implement and manage their information security programs, conduct security risk assessments, and secure their cloud infrastructure and applications.

Compliance Services

We help our clients meet legal, regulatory, industry, and contractual requirements (e.g., HIPAA, PCI DSS, GDPR, CCPA, etc.) by identifying and addressing compliance gaps, and establishing ongoing compliance programs.

Audit Readiness

Going through security audits and certifications such as SOC 2, HITRUST, or ISO 27001 is always stressful and takes resources away from key business processes and projects. Planet 9 helps organizations prepare and complete security audits, and gain necessary certifications.

Contact us

Phone: 888.437.3646

Email: info@Planet9Security.com

References

1. Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub. L. No. 104-191 https://www.govinfo.gov/app/details/PLAW-104publ191
2. U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/
3. U.S. Department of Health and Human Services. Summary of the HIPAA Security Rule https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
4. Omnibus Final Rule Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78, Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164). https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf
5. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009) https://www.govinfo.gov/content/pkg/FR-2010-07-14/pdf/2010-16718.pdf
6. International Organization for Standardization (ISO, 2018). Information technology — Security techniques — Information security risk management (ISO 27005:2018). https://www.iso.org/standard/75281.html
7. National Institute of Standards and Technology (NIST, 2012) Guide for Conducting Risk Assessment, SP 800-30 Rev. 1 https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
8. National Institute of Standards and Technology (NIST, 2017). Guide to Storage Encryption Technologies for End User Devices, SP 800-111, https://csrc.nist.gov/publications/detail/sp/800-111/final
9. National Institute of Standards and Technology (NIST, 2019). Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, SP 800-52, Rev 2. https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
10. National Institute of Standards and Technology (NIST, 2019). Guide to IPsec VPNs, SP 800-77 https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final
11. National Institute of Standards and Technology (NIST, 2008). Guide to SSL VPNs SP 800-113, https://csrc.nist.gov/publications/detail/sp/800-113/final
12. Federal Information Processing Standards (FIPS) 140-2 https://csrc.nist.gov/publications/detail/fips/140/2/final