puredome



What is HIPAA Compliance?
A Comprehensive Guide for Healthcare Organizations

A few years ago, patient access roles were handled by in-office staff.

But now, more and more healthcare organizations are changing their ways by substituting the front desk personnel with HIPAA-compliant Virtual Assistants instead. This innovation is catching on fast, with the VA market growing steadily at a rate of 28.5% annually. And it looks like it's going to keep up this momentum until at least 2031.

But there's one issue: Bringing virtual assistants on board also means dealing with security risks, which can keep healthcare CISOs and CSOs on edge. Here's your guide to understanding and ensuring HIPAA compliance for healthcare information.

HIPAA compliance is a living culture that healthcare organizations must implement within their business to protect the privacy, security, and integrity of protected health information. In addition to ensuring sensitive patient information is protected and secured, HIPAA compliance is critical for healthcare organizations to avoid legal and financial penalties.

Explore details about this U.S. regulation and learn about how to comply.

Insider Threats in Healthcare

As highlighted earlier, breaches often result from errors employees make—misplacing a device, falling prey to a phishing campaign, or engaging in informal discussions about patients with colleagues. HIPAA violations can easily occur, and insider threats may manifest as unintentional or malicious.

Notably, 56% of incidents involving insider threats are linked to the employee's negligence.

From March 2022 to March 2023, the healthcare industry experienced the highest average data breach cost, amounting to nearly **11 million U.S. dollars.**

What is the Health Insurance Portability and Accountability Act (HIPAA)?

The Health Insurance Portability and Accountability Act was initially focused on addressing insurance coverage gaps for individuals transitioning between jobs. Without this legislation, individuals would have risked losing their insurance coverage during job transitions.

Another objective was to guarantee the proper security of all data, preventing unauthorized individuals from accessing healthcare information. HIPAA is applicable within the United States and is governed by the Department of Health and Human Services' Office for Civil Rights (OCR).

History of HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 was passed by the U.S. Congress and signed into law by President Bill Clinton.

- Modernize the flow of healthcare information.
- Stipulate how personally identifiable information (PII) maintained by the healthcare and health insurance industries should be protected from fraud and theft.
- Address limitations on healthcare insurance coverage, such as coverage continuation despite job changes and coverage of individuals with pre-existing conditions.

HIPAA mandated national standards to protect sensitive patient health information from disclosure without patient knowledge or consent. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement this mandate.

The Privacy Rule contains 12 exceptions wherein patient data can be shared with other entities without patient consent. They include:

- Victims of domestic violence or other assault.
- Judicial and administrative proceedings.
- Cadaveric organ, eye, or tissue donation.
- Workers compensation.

Another key element of HIPAA compliance is the Security Rule, a subset of the Privacy Rule. This includes all individually identifiable health information that a covered entity creates, receives, maintains, or transmits electronically. Key elements of the HIPAA Security Rule include:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information.
- Detect and safeguard against anticipated threats to the security of the information.
- Protect against anticipated impermissible uses or disclosures.
- Certify workforce compliance.

Protected health information (PHI) is any demographic information that can be used to identify a patient or client of a HIPAA-beholden entity. Common examples of PHI include names, addresses, phone numbers, social security numbers, medical records, financial information, and full facial photos, to name a few.

Purpose of HIPAA

HIPAA was established to modernize the exchange of healthcare information and ensure the protection of Personally Identifiable Information collected by healthcare and insurance entities, safeguarding it from fraud and theft and preventing unauthorized disclosure.

Patient healthcare information is handled with increased sensitivity, allowing swift access by different healthcare providers. HIPAA laws and regulations mandate enhanced security measures to prevent data leakage. For comprehensive guidance on HIPAA regulations and compliance, you can refer to HIPAA Journal, an excellent resource with a detailed checklist for your compliance journey.

What Is Protected Health Information?

A crucial aspect of HIPAA compliance is understanding what constitutes Protected Health Information. According to the U.S. Department of Health & Human Services, Protected Health Information (PHI) refers to any individually identifiable health information held or transmitted by a covered entity or its business associate.

Any entity or individual handling Protected Health Information (PHI) must comply with HIPAA. PHI is formed when health data is linked with personally identifiable information, encompassing:

- Geographical identifiers
- Names
- Email addresses
- Phone and fax numbers
- Account numbers
- Medical record numbers
- Website URLs
- Vehicle information
- Social security numbers
- Retinal, voice prints, and fingerprints
- Device information, IP addresses
- Beneficiary numbers for health insurance
- Full face photographs
- Certificate and license numbers

When stored electronically, PHI is referred to as ePHI.

Ensuring the protection of PHI is crucial for myriad reasons, most fundamentally, patient privacy, data security, and compliance:

Patient Privacy

Ensuring patient confidentiality is critical to maintaining trust between healthcare providers and patients. Unauthorized access to personal health information can lead to embarrassment or stigma for individuals whose private details are exposed.



Data Security

Healthcare organizations store vast amounts of sensitive patient data that can be lucrative targets for cybercriminals seeking financial gain through identity theft or fraud schemes. Safeguarding PHI helps prevent unauthorized access and potential breaches.



Federal Compliance

Failure to comply with HIPAA regulations can result in severe penalties such as fines of up to $1.5 million per violation category per year (source), reputational damage, and even criminal charges.



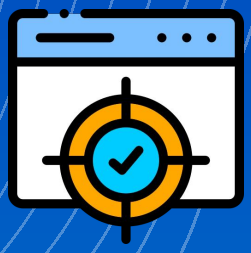
Identifiers of PHI

HIPAA regulations outline 18 specific identifiers that must be removed from health information to render it de-identified. Some common examples include:

- Name and address
- Social Security number (SSN)
- Date of birth (DOB)
- Email addresses, phone numbers, and fax numbers
- Medical record numbers or account numbers
- Fingerprints or facial images
- Certificate/license numbers
- Internet Protocol (IP) addresses
- Health plan beneficiary numbers
- Vehicle identifiers and serial numbers, including license plate numbers

HIPAA and PHI Compliance

In healthcare, HIPAA and PHI (Protected Health Information) compliance go hand in hand. HIPAA sets the rules for protecting PHI, which basically covers any health info that can identify someone. Following HIPAA is super important for healthcare groups to keep patient info safe and private. This means putting in place all sorts of safeguards—like admin tasks, tech tricks, and physical security—to stop unauthorized people from getting their hands on PHI. Making sure HIPAA and PHI compliance are up to the mark is key for keeping patient trust, dodging data leaks, and sticking to ethical standards in healthcare.



The Scope of HIPAA

Understanding which entities must comply with these regulations is crucial for maintaining data privacy and avoiding potential penalties. In general, there are two main categories of organizations that must be HIPAA-compliant:

Covered Entities

Business Associates

Covered Entities

Covered entities (CEs) are those directly involved in providing or administrating healthcare services. They include:

Medical Practitioners:

Such as physicians, dentists, pharmacists, and nurses; hospitals; clinics; nursing homes; and other healthcare providers delivering or administering medical care



Health plans:

These organizations offer health insurance coverage, such as HMOs (health maintenance organizations), PPOs (preferred provider organizations), Medicare/Medicaid programs, employer-sponsored health plans, and others.



Healthcare clearinghouses:

These businesses process nonstandard PHI into a standard format for electronic transmission between covered entities.

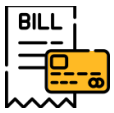


Business Associates

Business associates (BAs) are third-party service providers who access PHI while performing services on behalf of covered entities. Examples include:

Billing Companies:

Organizations responsible for processing claims or managing patient accounts.



Electronic Health Record (EHR) Vendors:

Companies that develop, host, or manage EHR systems for healthcare providers.



IT Service Providers:

Firms offering technical support, data storage, or cybersecurity services to covered entities.



Consultants and Auditors:

Professionals who access PHI while assessing a covered entity's operations and compliance status.



HIPAA Law & Regulations

HIPAA comprises the following regulatory rules:

Privacy Rule:

Defines how, when, and under what circumstances you can use and disclose PHI. Limits the use of patient information without prior consent. Patients can request copies of their health records and corrections.



Security Rule

Sets standards to protect electronic PHI (ePHI). Applicable to anyone working with ePHI. Requires risk assessments and audits by Security and Privacy Officers to identify threats to PHI integrity.



Breach Notification Rule

Mandates notifying the Department of Health and Human Services and affected individuals in case of a data breach. Press releases are required if over five hundred patients in a specific jurisdiction are affected.



Omnibus Rule

Part of the HITECH Act (2009) to encourage electronic health record use. Prohibits using PHI for fundraising or marketing without authorization.



Enforcement Rule

Focuses on determining fines for breaches—lower fines for negligence; significantly higher penalties for violations due to willful neglect.





What are the HIPAA Privacy and Security Rules?

Understanding HIPAA Privacy and Security Rules is essential for organizations that handle protected health information (PHI). These rules ensure that PHI is secure from unauthorized access or disclosure while preserving its confidentiality, integrity, and availability.

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards for protecting individuals' medical records and other personal health information. It applies to healthcare providers, health plans, healthcare clearinghouses, and their business associates who transmit electronic PHI (ePHI).



Covered Entities

Healthcare providers such as doctors, clinics, and hospitals; health plans, including insurance companies; and healthcare clearinghouses like billing services.



Business Associates

Third-party service providers that create, receive, maintain, or transmit ePHI on behalf of covered entities. Examples include IT contractors or cloud storage vendors.

The Privacy Rule requires covered entities to implement appropriate safeguards to protect patient privacy by limiting unnecessary access to PHI. They must also establish policies regarding using and disclosing PHI in various situations, such as treatment purposes or public interest matters like disease control.

HIPAA Security Rule

The HIPAA Security Rule specifically focuses on protecting ePHI by setting guidelines for implementing technical safeguards within an organization's IT infrastructure. This rule aims to ensure ePHI confidentiality while maintaining its integrity and availability to authorized users.

The Security Rule outlines three main safeguard categories:



Administrative Safeguards

Policies, procedures, and actions an organization's management takes to protect ePHI. Examples include risk assessments, workforce training programs, and incident response plans.



Physical Safeguards

Controls and policies to limit physical access to ePHI and related technology. These include facility access controls, workstation use, and device/media controls.



Technical Safeguards

Technical measures put in place to protect ePHI from unauthorized access or disclosure. Examples include encryption, access controls, and audit logs.

By following the Security Rule, covered entities and business associates can maintain the confidentiality and integrity of PHI while ensuring it remains available for authorized use when needed.

Physical and Technical Safeguards, Policies, and HIPAA Compliance

Physical Safeguards

Physical safeguards refer to the measures taken to protect the physical infrastructure housing PHI. These safeguards aim to control access to facilities and devices containing PHI, ensuring only authorized personnel can access sensitive information.

Some key physical safeguards include:

Facility Access Controls:
Implementing mechanisms like access cards, PIN codes, or biometric authentication to limit access to areas where PHI is stored or processed.



Workstation Use:
Establishing policies that govern how workstations should be used to prevent unauthorized access to PHI.



Device and Media Controls:
Implementing policies for the secure disposal of hardware and media containing PHI, such as shredding physical documents or securely wiping electronic storage devices.



Technical Safeguards

Technical safeguards involve the use of technology to protect PHI and control access to ePHI. They encompass various measures such as encryption, user authentication, and audit controls.

Some essential technical safeguards include:

Access Control:

Using unique user identifiers, passwords, or biometric authentication to ensure only authorized individuals can access ePHI.



Audit Controls:

Implementing software that tracks and records activity involving ePHI, allowing organizations to monitor access and detect unauthorized or suspicious behavior.



Data Encryption:

Using encryption techniques to protect ePHI from unauthorized access or disclosure, especially when transmitting data over networks or storing it on portable devices.



The Most Common Risks Associated with HIPAA

Unencrypted Data

While not mandatory, HIPAA highly recommends encrypting data. Even during a data leak, encrypted information remains inaccessible without proper authorization.



Unauthorized Access

Employees without proper authorization may access and review sensitive information. Establish and communicate security policies to ensure that employees are well-informed and compliant.



Keeping Unsecured Records

Employees may leave sensitive documents unattended at their desks or neglect to use passwords for accessing digital data. Ensure the workspace is secure and passwords are consistently employed within your company.



The Most Common Risks Associated with HIPAA

Sharing PHI

Awareness is key when it comes to sharing sensitive information. Employees may inadvertently share PHI with colleagues. Educate them on proper data handling, emphasizing that only authorized individuals should access such data.



Loss or Theft of Devices

Devices holding valuable information can be lost or stolen. Encrypting your data prevents unauthorized access, even if a device is lost.



Lack of Employee Training

Employees may not be aware that they are working with PHI, posing risks to the company and patients. Regularly educate employees on what PHI and HIPAA entail and the consequences of violations.





What Are Some Recent HIPAA Updates?

HIPAA regulations are not static; they continuously evolve to address emerging cybersecurity threats and technological advancements. It is essential for healthcare organizations to stay informed about recent updates to ensure compliance. Some of the notable recent updates include:



The Information Blocking Rule

The rule aims to promote interoperability and patient access to health information by preventing information blocking practices.

Information blocking refers to practices that unreasonably interfere with, prevent, or discourage access, exchange, or use of electronic health information (EHI). Covered entities and business associates must comply with the rule to ensure patients have timely access to their health information without unreasonable barriers.



Right of Access Initiative

OCR's Right of Access Initiative emphasizes the importance of providing timely and easy access to medical records. The initiative clarifies that patients have the right to obtain their health information promptly and without unreasonable delays.

Under this initiative, covered entities must provide patients with copies of their medical records within 30 days of the request (with certain exceptions) and charge only a reasonable cost-based fee for the copies.

Guidance on Ransomware Attacks

In recent years, ransomware attacks have targeted healthcare organizations with increasing frequency. The U.S. Department of Health and Human Services (HHS) issued guidance on the growing threat of ransomware and the importance of implementing robust security measures to protect ePHI.

Healthcare organizations are advised to have proper backups, strong access controls, and incident response plans in place to respond effectively to ransomware attacks and other cybersecurity incidents.



Telehealth Flexibilities

The COVID-19 pandemic led to a surge in the use of telehealth services to provide remote healthcare consultations. In response to the pandemic, the HHS temporarily relaxed certain HIPAA enforcement rules related to telehealth to facilitate remote patient care.

Telehealth flexibilities allowed the use of popular video communication platforms (e.g., Zoom, Skype) for telehealth consultations, even if they were not fully HIPAA-compliant. The flexibilities aimed to ensure patients could access essential healthcare services while reducing potential exposure to the virus.

While the specific telehealth flexibilities may have evolved or ended by 2023, it is essential for healthcare organizations to stay updated with the latest guidance from the HHS and OCR regarding telehealth practices.



How Do You Secure Health Information for HIPAA Compliance?

Understanding and addressing the key components of the HIPAA laws and regulations is essential for ensuring the integrity, confidentiality, and availability of health information while meeting the compliance standards set forth by this vital legislation.

Complying with HIPAA involves navigating a comprehensive set of regulations to safeguard the security and privacy of individuals' health information. To adhere to HIPAA guidelines, organizations must establish robust measures for safeguarding electronic protected health information (ePHI).

Advanced Encryption

Ensure traffic encryption within your company's network using AES 256-bit encryption, providing a robust defense against unauthorized access to data. This crucial security measure aligns with HIPAA's stringent requirements for protecting electronic protected health information (ePHI). Additionally, adopt comprehensive security policies and designate authorized personnel for accessing PHI.



Robust Authentication and Authorization

Implement stringent controls for authentication and authorization. Restricted to approved individuals within specific organizations and teams, you can ensure that only authorized personnel can access or grant specific information and permissions. This aligns seamlessly with HIPAA's mandate to control access to ePHI, bolstering overall data security.



Secure Business VPN

A business VPN imposes restrictions on access, introducing an additional layer of control. This stringent limitation guarantees authorized personnel access to sensitive information exclusively through secure channels, perfectly aligning with HIPAA's emphasis on controlled access to ePHI.



Secure Communication Channels

Utilize encrypted communication channels and secure messaging platforms to transmit PHI securely between healthcare providers and virtual assistants. Implement technologies that ensure end-to-end encryption to prevent unauthorized access.



Access Control Measures

Implement strict access controls to limit PHI access only to authorized personnel. Utilize role-based access control (RBAC) systems to ensure that each virtual assistant can only access the information necessary for their tasks.



Business Associate Agreements (BAA)

Establish Business Associate Agreements with virtual assistant service providers to ensure they understand their responsibilities regarding PHI protection and HIPAA compliance. These agreements outline the terms and conditions for handling PHI and establish liability in case of breaches



Zero Trust Network Access (ZTNA)

Implement ZTNA solutions to enforce strict access controls and verify user identities before granting access to PHI. ZTNA ensures that every access request is authenticated and authorized, regardless of the user's location or network connection. This reduces the risk of unauthorized access to sensitive data.



Regular Audits and Assessments

Conduct regular audits and assessments of virtual assistant systems and processes to identify any potential security vulnerabilities or compliance gaps. Address any issues promptly to maintain compliance and mitigate risks.



How to Simplify HIPAA Compliance with PureDome

Amid the increasing prevalence of remote and hybrid work arrangements, achieving compliance with regulatory standards has become progressively intricate. As an integral component of PureDome, our primary commitment centers around furnishing a comprehensive array of top-tier cybersecurity solutions, guiding you in attaining and sustaining compliance standards.

1. Ensure **secure data transfer** with advanced technologies, using **Shared Gateways** and **VPN protocols** for encryption and IP masking.
2. Utilize a **HIPAA-compliant solution** for secure remote access through a **Device Posture Check** and enforce security rules.
3. Adopt a **zero-trust approach** for data under compliance directives. Implement additional measures like **2FA and SSO** for robust network control.
4. Proactively prevent incidents with **network activity monitoring** and maintain **secure communication channels.**

Here is how PureDome can help you achieve compliance.

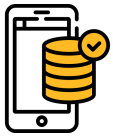
Continuous Data Encryption:

Utilizing advanced technologies, PureDome consistently ensures the confidentiality of data during its transfer. Shared Gateways, equipped with advanced VPN protocols, ensure encrypted data transfer and IP masking on the open internet.



Device Posture Checks:

Continuous inspection of devices enhances your capacity to assess the overall security and health of the network. Our HIPAA-compliant network security solution fortifies secure remote access with a Device Posture Check. Evaluate users' devices based on predefined security rules and provide notifications for non-compliant devices.



Zero Trust Approach:

To secure data governed by compliance directives, PurrDome adopts a zero-trust approach. This involves implementing additional confirmation measures, such as 2FA and SSO, to ensure robust and secure network control.



Effective Monitoring and Logging:

Monitor network activity and maintain secure communication channels to prevent and investigate incidents. PureDome facilitates scrutinizing usage logs, identifying users of secured connections, and detailing the timing of their usage.



Conclusion

HIPAA compliance is a pivotal element within the healthcare sector, incorporating an extensive array of standards and regulations crafted to protect patient privacy, secure electronic health information, and advance administrative simplification. This regulation is crucial in safeguarding individuals' sensitive health data, fostering trust in the healthcare system, and enhancing overall operational efficiency. Compliance with the standards articulated in HIPAA enables healthcare organizations to fulfill legal obligations and plays a critical role in fostering a secure, patient-centric, and streamlined healthcare environment.