

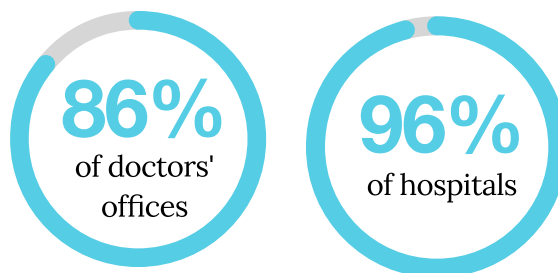
A Guide to

Securing Healthcare Information with HIPAA Compliance

Fast-track your compliance efforts with a secure, reliable, and quick HIPAA-compliant network security solution.

Introduction

Before the pandemic, only 11% of U.S. patients utilized digital health services; however, this figure has [surged to nearly 50%](#) as telehealth solutions become increasingly popular. According to the [American Hospital Association](#), even prior to the pandemic, 76% of hospitals offered some form of telehealth, with this number experiencing substantial growth. Electronic Health Records (EHRs) are now prevalent, used by



The transition to telehealth presents both promising and concerning aspects. While it offers significant opportunities to enhance patient care, the abundance of data simultaneously expands the potential attack surface, raising security concerns. Therefore, it is crucial for healthcare companies to establish and implement best practices that align with current HIPAA standards, ensuring ongoing protection for patients

Are you well-versed in the requirements for achieving and maintaining HIPAA compliance?

Read on for insights into strengthening security and compliance posture.

HIPAA: A Refresher



HIPAA, an abbreviation for the Health Insurance Portability and Accountability Act, is a comprehensive legislation governing healthcare and health insurance entities in the United States, along with other designated "covered entities," concerning the handling of "protected health information" (PHI).



In the U.S., HIPAA establishes regulations dictating how health insurers and healthcare providers collect, safeguard, and share patient information. This federal legislation establishes the baseline for health data privacy compliance nationwide. Notably, individual state legislatures possess the authority to adopt regulations that surpass HIPAA, thereby elevating the compliance standards for health information protection within those states.

Here is a summary of the technical safeguards within HIPAA and their respective components.

Technical Safeguards

| Technical Safeguards | Description | PureDome Capabilities/Solutions |
|------------------------------|--|---|
| Access Controls | Implement technical policies for authorized access, unique user identification, emergency access modes, and automatic log-off. |  |
| Audit Controls | Introduce mechanisms to record and inspect access in information systems containing ePHI. | — |
| Integrity Controls | Enforce policies to prevent improper alteration or destruction of ePHI. | — |
| Transmission Security | Implement technical security measures, including encryption, to guard against unauthorized access to transmitted ePHI. |  |

The HIPAA Security Rule: Are you in Compliance?

The HIPAA Security Rule serves as a tool to enhance your confidence in addressing this concern. But what does the HIPAA Security Rule entail?

Extending the scope of the HIPAA Privacy Rule, the HIPAA Security Rule encompasses electronic protected health information (ePHI). It mandates the proper safeguarding of all ePHI, whether at rest or in transit, to prevent unauthorized access (breach).

The rule is crafted flexibly to address all security aspects without mandating specific technologies or procedures. Each organization is responsible for determining its unique security needs and devising strategies to fulfill them.

Applicable to covered entities and their business associates (BAs), the HIPAA Security Rule requires that they establish written business associate agreements (BAAs) when engaging with vendors or organizations that will access ePHI. A BAA outlines how ePHI will be utilized, disclosed, and protected.

The HIPAA Security Rule with PureDome

Here is how PureDome addresses the components of the HIPAA Security Technical Safeguards.

Transmission Security



Enhanced Encryption

VPN encryption provides an additional layer of security crucial for healthcare data protection, particularly under HIPAA regulations. When accessing sensitive data over public or untrusted Wi-Fi networks, malicious actors can eavesdrop and steal credentials from authorized sessions, impersonating legitimate users to access PHI. This is where a HIPAA-compliant VPN ensures that only authorized personnel can access patient records. Additionally, the Device Posture Check (DPC) can enhance security by ensuring that only compliant devices access the healthcare network, reducing the risk of data breaches and maintaining compliance.

Access Controls



Robust Authentication and Authorization

Within PureDome's admin panel, robust authentication and authorization controls are in place. Limited to approved individuals within specified organizations and teams, this functionality guarantees that only authorized personnel can access or grant specific information and permissions. This aligns seamlessly with HIPAA's imperative to control access to ePHI, reinforcing overall data security.

Transmission Security

Access Controls



Secure Business VPN

PureDome's business VPN restricts access, adding an extra layer of control. This stringent limitation ensures that sensitive information is accessed solely by authorized personnel through secure channels, perfectly aligning with HIPAA's emphasis on controlled access to ePHI.

How can Covered Entities & BAs Achieve Compliance with PureDome?

Amid the rising prevalence of remote and hybrid work, achieving regulatory compliance on a broader scale has become increasingly complex. As an integral part of PureDome, our primary dedication revolves around delivering a comprehensive suite of high-quality cybersecurity solutions and assisting you in achieving and upholding compliance standards.

Here is how PureDome can help you achieve compliance.



Continuous Data Encryption

Employing advanced technologies, we consistently uphold data confidentiality during its transfer. Shared Gateways, functioning with advanced VPN protocols, guarantee encrypted data transfer and mask your IP on the open internet.



Device Posture Check

Continuous device inspection enhances your ability to evaluate the overall security and health of the network. Our HIPAA-compliant network security solution reinforces secure remote access with Device Posture Check. You can assess users' devices based on predefined security rules and receive notifications regarding non-compliant devices.



Effective Monitoring and Logging

You can proactively prevent and investigate incidents by monitoring network activity and ensuring secure communication channels. PureDome facilitates the inspection of usage logs, identifying users of secured connections and the timing of their usage.



Zero Trust Approach

To safeguard data protected by compliance directives, PureDome adopts a [zero-trust approach](#). This involves enforcing additional confirmation steps, including 2FA and SSO, to maintain robust and secure network control.

Simplify your Compliance & Security Journey

Key features of PureDome's HIPAA-compliant network security solution include:



Secure Remote Access: Guarantee [secure network access](#) for remote and hybrid work environments, minimizing health data risks through our Secure Remote Access from all endpoints.



Streamlined Access Controls: Ensure that only authorized users can access Protected Health Information (PHI) with our simplified network access controls.



256-bit AES Encryption: Streamlined Access Controls: Ensure that only authorized users can access Protected Health Information (PHI) with our simplified network access controls.

Your HIPAA Compliance Journey Begins Here

The imperative for healthcare organizations is evident – prioritizing data security is essential to safeguard patient information and ensure compliance with regulatory standards. PureDome provides healthcare professionals with a robust and dependable HIPAA-compliant VPN solution, meeting the highest encryption and security software requirements.

With customers like [HelloRache trusting PureDome as their cybersecurity partner](#), discover how you can ensure your organization can uphold the highest levels of HIPAA compliance for remote employees with a zero-trust approach.

[Book a demo](#) to learn more, or [get started for free today](#).

Sources:

<https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>

<https://www.aha.org/factsheet/telehealth>

<https://hbr.org/2020/06/its-time-for-a-new-kind-of-electronic-health-record>