



How Safetica Helps to Comply with HIPAA

Version: 2022-08-08

Introduction to HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was initially designed to improve the portability of insurance coverage for individuals who were between jobs. Before this law, employees faced the risk of losing their insurance coverage for the period between jobs.

Another goal was to ensure that all data was properly secured, and no unauthorized individuals could access healthcare data.

HIPAA applies to organizations in the United States and is regulated by the Department of Health and Human Services' Office for Civil Rights (OCR).

Purpose of HIPAA

HIPAA was created to modernize the flow of healthcare information and to make sure that Personally Identifiable Information gathered in healthcare and insurance companies are protected against fraud and theft and cannot be disclosed without consent.

Patients' healthcare information is treated more sensitively and can be quickly accessed by various healthcare providers. HIPAA regulations require that records are better secured and protected against leakage.

What is Protected Health Information (PHI)

PHI is created when any health data is combined with personally identifiable information, such as name, email address, account numbers, medical record number, full face photographs, Social Security numbers, etc. When PHI is stored electronically, it's called ePHI.

The scope of HIPAA

There are several entities that work regularly with Protected Health Information and therefore must adhere to the Health Insurance Portability and Accountability Act:

- Healthcare providers
- Health plans
- Healthcare clearinghouses
- Business associates

You can find detailed information about HIPAA in our blog [article](#).



Related **Challenges** and how **Safetica** helps to meet them

1. Keeping PHI private and confidential

The Privacy Rule requires you to secure patient records containing PHI, so they aren't readily available to those who don't need to see them.

Using content inspection with OCR, Safetica can automatically classify PHI data and enforce DLP policies that define where such data can be stored, where they are allowed to flow and how. This ensures secure storage is enforced and access to PHI can be limited to critical personnel only.

Depending on the DLP mode that the Safetica solution is set to, it can either block the risky activity, notify the user (and admin), redirect employees to the organization's security guidelines, or allow them to justify the restricted operation.

2. Sharing Information with other Health Care Professionals

The Privacy Rule requires you to secure patient records containing PHI when they are shared to other Health Care Professionals.

Safetica facilitates the management and control of where sensitive data can be stored and the destinations (data channels) or peripherals from which data can leave a department or organization. The flow of PHI data that Safetica automatically detects and classifies can be controlled by simple DLP policies.

DLP policies can prevent PHI from leaving an organization. Additionally, a secured perimeter (zone) can be defined to specify authorized recipients and third parties who are allowed to work with the data without restrictions. All of this is subject to continuous monitoring, and all actions, blocked or allowed, are recorded for audits and purposes of investigation.

An optional feature also allows specific users to override an existing, broad security policy. Using this DLP mode, a user must provide a business justification, which is then recorded and reported to the security personnel. This allows selected users to work around restrictive security policies in case of urgent need, but also communicates to the security personnel what was required and why.

3. Sharing information with family members

The Privacy Rule lets you communicate with identified and approved family members as long as you use safeguards to protect the privacy and confidentiality of patients' PHI.



The Safetica solution offers an option to whitelist authorized, but still monitored, destinations and recipients to receive PHI and other sensitive data. For more details, see the previous section.

4. Breach notifications

When you experience a PHI breach, the HIPAA Breach Notification Rule requires you to notify affected individuals, HHS, and, in some cases, the media.

In the event of an actual or attempted data security incident, the real-time email alert system in Safetica notifies the appropriate personnel. It promptly reports the incident and provides sufficient detail so they can assess the impact of the situation and take follow-up actions.

Safetica also provides extensive audit records on operations performed with sensitive data. This helps to identify the depth of the breach, the sensitive documents concerned, and the individuals affected.

Using API integration, all records can also be sent to SIEM or data analytic tools, e.g., Power BI or Tableau.

5. Encryption of PHI data stored at endpoint devices

HIPAA requires several safeguards to protect PHI when stored in data storage. One of these requirements is encryption.

Safetica helps organizations manage storage encryption (Microsoft BitLocker), thus protecting data at rest. Encryption is centrally managed in the Safetica management console, with encryption keys securely distributed across secure endpoint devices, eliminating the need to share them between users.

Key Use Case

Healthcare Software Provider

A leading US provider of practice management applications and medical billing and automation software for healthcare organizations needs to protect patient data and comply with HIPAA.

Problem: The company processes a huge amount of data that can appear anywhere in the environment. Therefore, they need to know where the data is, who worked with it, and how. A ticketing system for this medical billing software can also process screenshots and other customer requests that could contain patient data that requires appropriate protection.

Solution: The combination of Safetica ONE Enterprise with the UEBA module provides unified yet flexible data discovery and classification. Content policies using built-in templates




for PII and HIPAA will give the customer an overview of where the sensitive data is and where it flows.

Configuration of multiple Safe zones will help to define specific areas where it's safe to work with data without hard restrictions. Device control only lets users connect company-approved USB devices to their computers. All data needs to be encrypted and the Bitlocker encryption can be managed from the central console in Safetica.

Safetica can classify all downloads from the ticketing system server and only allow uploads back to the system or protected network drive.

Results: The company continually meets HIPAA compliance requirements. With Safetica, the company understands where the sensitive data can appear and can control how the data is allowed to move within their systems. Safetica ONE Enterprise also provides integration options with Microsoft 365 and Microsoft Information Protection. Data security notifications from Safetica ONE are sent to SIEM for further analysis. The rest of the logs are kept in Safetica Management Console.





Excellent Data Protection Made Easy

safetica

© Copyright All rights reserved. Safetica and the Safetica logo are registered trademarks. All trademarks are the property of their respective owners.

www.safetica.com