SAFE®

Use Case: HIPAA Compliance

How SAFE helps Healthcare and medical information organizations solve problems and improve business functions.

Paperclip and HIPAA Compliance Overview

Paperclip Inc. is a 32-year-old SaaS innovator providing solutions focused on critical content, documentation, and security. Paperclip realized that to truly secure its clients' data, it needed to keep data encrypted while in use—so SAFE® was born.

SAFE is a breakthrough encryption-in-use solution that ensures valuable data is never decrypted, while remaining fully searchable at high speeds. For the Healthcare market, securing customer data while continuing regular business functions is critical, yet most companies are not able to do so with current solutions.

The Challenge

Health Insurance Portability and Accountability Act (HIPAA) data requirements manifest in two ways: daily operations and archive. The archive requirement is six years for Covered Entities (CE) and Business Associates (BA) when containing Personal Identifiable Information (PII) and Personal Health Information (PHI). Because of this requirement, these organizations become the perfect candidates for a mega-breach, just as Premera Blue Cross and Excellus Health Plan experienced. And in each of those cases, they were fined more than five million dollars and the final breach cost them an estimated $200 million each.

The reason they were exposed is because, in healthcare, archive data must be searchable. HIPAA encourages organizations to take advantage of technologies that provide individuals with immediate access to their health information. While that's great for patients and health workers—how do they keep the information secure while allowing it to be searched?

The practical solution is to encrypt the data, but most of today's encryption solutions don't enable search while encrypted. So, the data is then decrypted during the search process and therefore exposed. And the data used for daily operations is in plaintext, which threat actors can easily access and steal. Access controls and perimeter security are just obstacles to overcome on their way to stealing your data—they're not likely to stop them.

The Solution

The best way to keep healthcare information safe is to always encrypt the data with strong NIST encryption standards. This way when the threat actors reach the data, it has no value.

In the past, if the data stolen was encrypted you were in "Safe Harbor" which was not considered a breach. Today, you would need to prove that the encryptions keys were not also exposed and if you can't, it's a breach. Therefore, protecting the data must go beyond encryption.

The Result

Paperclip SAFE goes beyond encryption. SAFE enables privacy by using two separate key vaults, one for the data holder and one for the data owner, reducing the likelihood of accessing encryption keys. SAFE also uses machine learning to detecting data threats and responses.

And if the SAFE encrypted data and encryption keys are stolen, the data is *still* not exposed because of Paperclip's patented shredding technology. Threat actors only end up with meaningless, unique shreds of data that does not expose its real content—and therefore is not a breach.

And best of all, SAFE provides unparalleled speed of access for encrypted data, which is a brand-new capability in the market. Healthcare organizations can rest easy knowing their PII & PHI data is SAFE and out of harms way from threat actors.

Paperclip

One University Plaza Hackensack, NJ 07601
201.525.1221

Paperclip.com