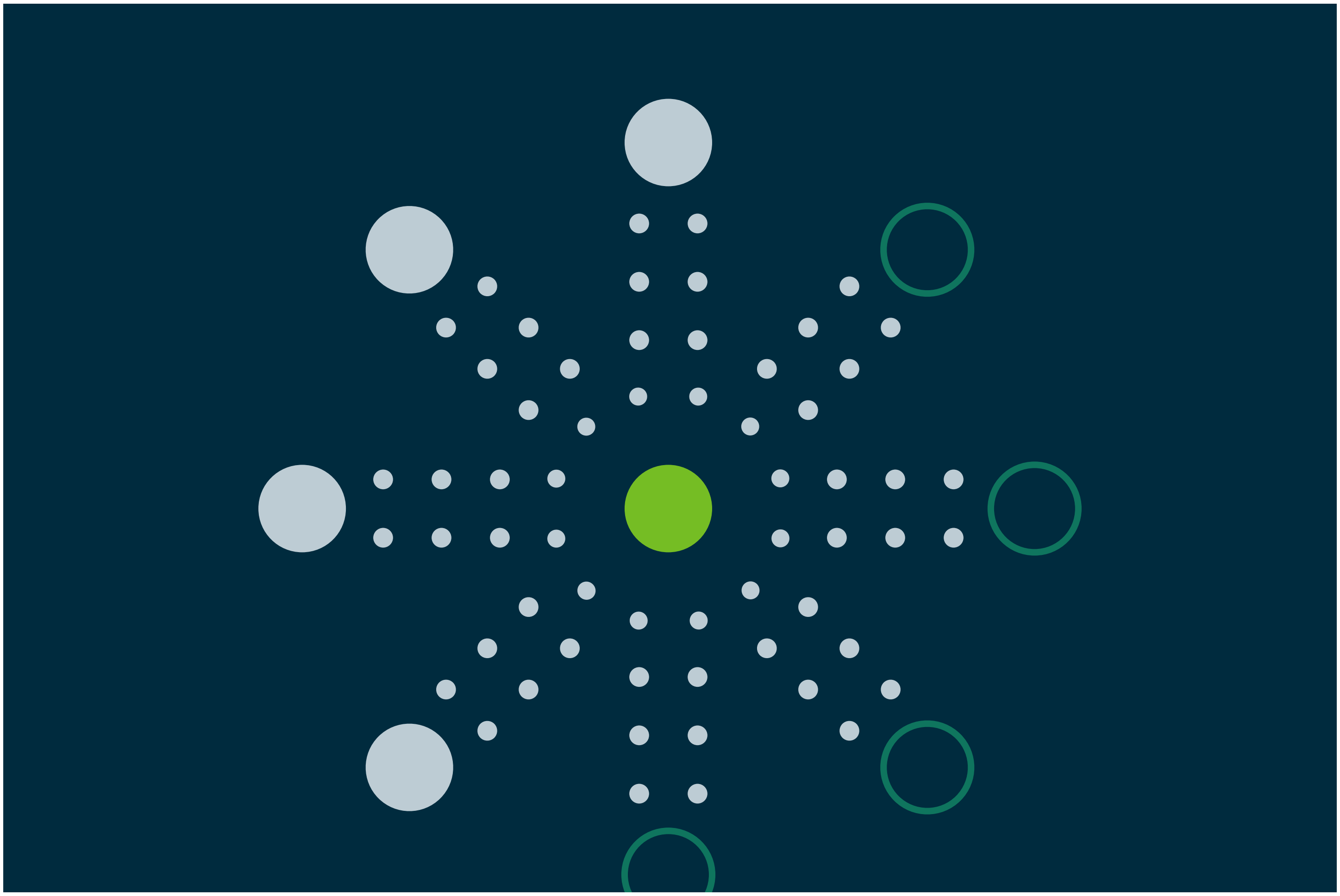
Collibra

Whitepaper

Collibra and HIPAA



Overview

Back in the early 90s there were no established rules governing the security and privacy of healthcare data. During the rapidly expanding era of the internet, Congress decided to pass a law to standardize protections around healthcare data. It passed the Health Insurance Portability Act (HIPAA) in 1996 which required the Department of Health and Human Services to develop these objectives. In 2003, they authored what are known as HIPAA Privacy Rule and the HIPAA Security Rule. The Security Rule details a set of technical security standards for organizations that use Protected Health Information (PHI). The Privacy Rule compliments the Security Rule and provides rules around the use and disclosure of PHI. In 2006, the US Department of Health and Human Services (HHS) issued the HIPAA enforcement rule which provides rules and procedures for investigating potential HIPAA disclosure along with monetary penalties for confirmed HIPAA violations. The final significant update to the Act came in 2013 when the law protections were expanded to include not only for the original holders of the HIPAA data (Covered Entities), but also to entities granted access to that data by the covered entity (Business Associate).

Collibra and HIPAA

In an effort to provide confidence in our data security to our Healthcare customers, Collibra has achieved an attestation of our adherence to the HIPAA Security Rule. We maintain this attestation to ensure compliance with any BAA commitments and allow our Healthcare customers to use features such as our Sampling and AI/ML-based Data Classification.

HIPAA Security

The HIPAA security rule divides its standards into 3 sets of rules: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Collibra adheres to these rules and we map out policies and controls to each of them to ensure compliance.

Below are some examples of our policies and procedures and how they map to HIPAA compliance

Administrative Safeguards

- Comprehensive Security Awareness program that offers annual training to all employees along with specialized training for developers
- Detailed Security Incident Management Process to ensure client data stays safe
- Security Policies and Procedures that are updated yearly at a minimum
- Background checks prior to hiring

Physical Safeguards

- Datacenters have industry standard SOC 1 and 2 for physical security procedures
- All office locations are secured and have ISO 27001 compliance
- All employee workstations have hard drive encryption and remote wipe ability

Technical Safeguards

- Strict access control around our Cloud accounts to ensure infrastructure security and accountability
- Access to Cloud systems is secured by multifactor authentication methods
- All data is encrypted in transit and at rest using the latest industry standards like TLS and AES
- Auditing is enforced for any high privileged accounts and for all major changes in the infrastructure.

Collibra – built securely for the future

Collibra's cloud-based platform is built for both today's digital transformation and the data challenges of tomorrow. This includes both private and public organizations that can utilize our world class data intelligence capabilities. Our commitment to HIPAA shows this and we will continue to support the security requirements of our public-sector partners. Security is at the core of everything we do, and federal agencies will be able to use Collibra in the cloud with confidence.