Secure Protected Health Information and Support HIPAA Compliance

Virtru's end-to-end encryption, security settings, granular access controls, identity authentication, and one-click secure patient access helps you meet compliance and go beyond it to meet your duty to protect sensitive data.

HIPAA Data Security Requirements

The Health Insurance Portability and Accountability Act (HIPAA) includes a Security Rule to protect how electronic PHI (ePHI) is created, received, used, or maintained. The Security Rule includes required and addressable safeguards to maintain the integrity, availability, and confidentiality of ePHI, such as:

- ePHI – whether at rest or in transit – must be encrypted to NIST standards once it travels beyond internal firewalled servers and render data unreadable and unusable if a breach occurs.
- Use activity logs and audit controls to register attempted access to ePHI.
- Empower employees to be secure, train on procedures governing access to ePHI, and help prevent human error.

Unlike solutions using TLS encryption that only encrypts data in transit, Virtru protects data from creation to storage to internal and external sharing.

Virtru uses encryption algorithms that comply with FIPS 140-2, is FedRAMP authorized at the moderate impact level, and adheres to the security controls defined by NIST SP 800-53. Virtru cannot access your protected data at any time.

Virtru is a Crucial Part of Your Solution to Help Meet HIPAA Compliance

End-to-End Encryption

Protect data throughout its lifecycle, require authentication or share data directly with patients via one-click secure access, and go beyond email to encrypt data in Google Drive and SFDC apps.

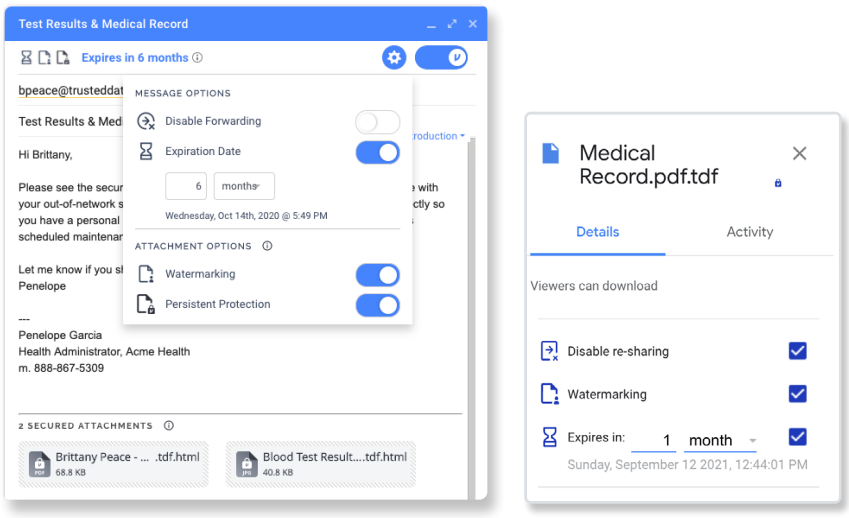
Maintain Data Visibility

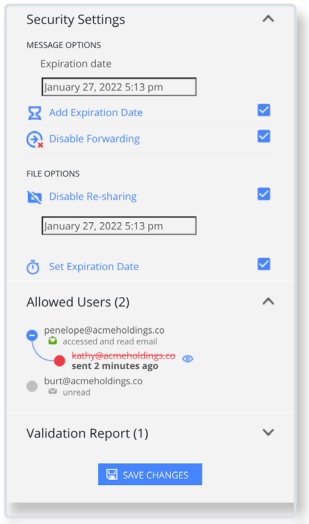
Use Virtru's Control Center and audit logs to see who has attempted to access data at any point in time, track where your data travels, and take action to reduce/ mitigate breaches.

On-Demand Access Controls

Revoke access and adjust access controls to maintain complete ownership over your data. Only encrypt data that needs to be protected with our HIPAA DLP rule pack and create your own rules.

Seamless Data Protection and Control for the Infrastructure, Software, and Devices You Use Today





Set Encryption Rules & Add Access Controls

Easily integrate into daily workflows and prevent human error by automatically enabling encryption or alerting users who handle HIPAA-protected data to secure emails and files. Revoke messages, disable forwarding, set expiration, watermark files, and maintain persistent control of files. Default “encrypt & upload” as the option for users adding documents in Google Drive.

Support Data Governance Through Granular Audit Trails

View when and where messages and files have been accessed and adapt controls for evolving workflows and collaboration requirements.

Proven Platform to Support Compliance with Google and Microsoft

Trusted Data Format

Use data-centric encryption to protect data beyond the original recipient and ensure no third party (including Virtru) can access your data.

Audit and Access Logs

Check granular views of data access to see if a breach occurred, or did not occur, to quickly complete detailed audits and understand risks.

Data Protection Gateway

Extend encryption and access controls into any of the applications that power your sensitive, digital healthcare workflows.

More than 6,000 customers trust Virtru for data security and privacy protection

ComForCare HOME CARE · Genesis · OSCAR · omada · REHAB Hospital of the Pacific

virtru

Learn how Virtru helps you meet HIPAA compliance and supports your organizational goals for data protection: **virtru.com/contact-us**