Enabling HIPAA Compliance with Virtru

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) gives directives for organizations to better safeguard individuals' protected health information (PHI).

HIPAA guidelines protect a wide range of information, so most organizations — even outside of the healthcare industry — must take steps to stay compliant.

Who does HIPAA affect?

Any company that handles this information is responsible for protecting it in accordance with HIPAA guidelines:

- **Healthcare Organizations:**
  - Hospitals
  - Counseling Centers
  - Medical facilities
  - Doctor's Offices
- **City and County Governments**
  - Health and Human Services Departments
  - Welfare Departments
  - City/County Assistance Offices

- **State Governments**
  - Health and Human Services Depts.
  - Medicaid Programs
  - Depts. of Public Social Services
  - Depts. of Supportive Services
- **Insurance firms**
- **Nonprofits providing health or social services**
- **Universities**
  - Student health providers
  - University hospitals
  - Medical and Dental Schools
  - Offices of Student Life
- **K-12 school districts**
  - School nurses
  - Teachers of students with medical conditions

Additionally, all corporate HR departments must comply with HIPAA, regardless of industry, because they process employee benefit and health insurance information.

PHI is a broad term, so HIPAA covers a broad range of organizations. PHI includes:

- Names
- Social Security numbers (SSNs)
- Medical record numbers
- Birthdates
- Medical symptom descriptions
- Insurance plan beneficiary numbers
- Medical device identifiers and serial numbers
- Fingerprints
- Medical history reports
- ICD-9 codes, and other unique identifying numbers, characteristics, or codes

What Are the Encryption Requirements?
How Does Virtru Help?

The U.S. Department of Health and Human Services (HHS) defines four categories of technical safeguards required for HIPAA compliance:

- Access controls
- Audit controls
- Integrity person or entity authentication
- Transmission security

Virtru's encryption software is certified HIPAA compliant because it meets or exceeds each of these technical safeguards:

Topic	HIPAA Requirements	Relevant Virtru Features
Transmission Security	Transmission of ePHI must be protected — either with integrity controls, encryption, or both.	Client-side encryption with network data protection option; data loss prevention (DLP) rules for automatic encryption
Audit Controls	Administrators must be able to track accesses and edits to ePHI for auditing purposes.	Message read receipts; message forwarding audit
Access Controls	Administrators must be able to control who can access ePHI, and when.	Message revocation; message expiration; forwarding control; DLP
User Authentication	Users must use authentication to be allowed access to ePHI	Supports OAuth, SAML, and Federated IDs, as well as email verifications
Breach Prevention	Employees should not send ePHI outside of allowed areas — on purpose or by accident.	Message revocation; message read receipts
Emergency Access	ePHI must be always accessible, even when main servers are down.	Signed Business Associate Agreement (BAA) includes an emergency access plan for continuing critical business processes

Going Beyond the Requirements

In addition to these requirements, Virtru provides other valuable security and control capabilities for organizations looking to comply with HIPAA:

- **Persistent Access Control –** Revoke access to PHI shared inadvertently, or set message expiration periods when communicating with recipients who do not require long-term access to patient or employee health information.

- **Message Audit –** See when messages are forwarded and revoke access at any point to ensure that only authorized recipients can access PHI.

- **Customer-Hosted Encryption Keys –** Virtru's Customer Key Server (CKS) allows agencies and other organizations to choose where their encryption keys are located. As a result, they can ensure that keys stay within the United States, while also preventing third party cloud providers from ever accessing their unencrypted data.

- **Search and E-Discovery –** Unlike S/MIME and PGP, Virtru's client-side encryption keeps messages searchable and exportable for Freedom of Information Act requests, audits, or other e-discovery requirements.

Have more questions about HIPAA encryption requirements?

Contact sales@virtru.com today to speak with one of our compliance experts.

More Than 6,000 Organizations Have Made the Switch to Virtru

Mount Sinai

ROSALIND FRANKLIN UNIVERSITY of MEDICINE AND SCIENCE

Collective Health

PATIENTPING