How Code42 Helps Organizations Maintain HIPAA Compliance

Code42 endpoint data protection supports customer compliance requirements with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule for the protection of sensitive health information.

What is HIPAA?

HIPAA is United States legislation that set the standard for the protection of sensitive patient data. More specifically, the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) established a national set of security standards for protecting health information that is held or transferred in electronic form (electronic Protected Health Information, or ePHI), to ensure the confidentiality, integrity and availability of all ePHI created, received, maintained or transmitted.

Code42 and HIPAA

Code42 can be configured to support compliance with HIPAA by following these steps:

1. **Enter into an agreement.** A Business Associate Agreement (BAA) must be signed with Code42 before a Code42 environment can be seen as supporting HIPAA compliance. The customer is responsible for developing and enforcing their own policies for using Code42 in a HIPAA-supported manner.
2. **Configure your instance.** We recommend using the "Compliance Settings" feature, which automatically configures the settings to support compliance. However, some customers will need to configure the settings manually, as explained on Code42 HIPAA Support Page.

How Code42 Gives You Control of Your Data

Code42 endpoint data protection delivers several key functionalities that play a vital role in supporting HIPAA compliance:

1. **Collect and control your endpoint data**

   Your employees and end users create and move an incredible amount of data on a daily basis. More than half of this data now lives exclusively on endpoint devices—laptops and desktops. In today's world, these devices (and the data that resides on them) can sit outside the traditional perimeter and beyond the visibility of traditional data security tools. Code42 solves this challenge, automatically collecting and securely backing up all endpoint data every 15 minutes. This is the starting point of a comprehensive data security and data control strategy.

2. **Maintain storage where you need it**

   Code42 gives you the flexibility to choose your deployment option—and delivers the same functionality and data security in both cloud and on-premises deployments. Most importantly, Code42 gives you the ability to control where your data lives, no matter your deployment.

3. Maintain complete data security

We protect all customer data with end-to-end encryption: 256-bit AES encryption to secure data at rest and 256-bit Transport Layer Security (TLS) 1.2 encryption to secure all data in transit.

In addition, Code42 enables customers to control management of encryption keys, including options where no Code42 staff ever has access to customer backup data. Advanced backup and deduplication technologies collect, store and restore data without Code42 staff ever accessing the content—it's all ones and zeroes to us.

4. Gain visibility, monitor data movement and spot risk sooner

At Code42, we believe HIPAA compliance is about more than checking boxes; it's about choosing solutions that enable your organization to mitigate the risk of ePHI falling into the wrong hands. By automatically and continually collecting all endpoint data, Code42 delivers comprehensive visibility of an organization's most sensitive and valuable data.

See how your employees move data—from servers to endpoints, endpoints to endpoints, endpoints to external devices or to public cloud storage. Leverage this powerful data visibility to enable a proactive and intelligent approach to data security and protection. Establish baselines of normal individual user activity and detect deviations or unusual activity. In short, spot anomalies sooner. Take action faster.

Security Features by Deployment

Deployment Model	Authority in AWS, Storage in Code42 Cloud	Authority On-Prem, Storage in Code42 Cloud	Authority and Storage with Customer	Authority and Storage in Code42 Cloud	Hybrid (storage in multiple locations)	Managed Private Cloud
Is data encrypted at rest?	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256
Is data encrypted in transit?	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256	Yes, AES-256
Does Code42 have access to data?	No	No	No	No	No	No
Who holds encryption keys?	Customer	Customer	Customer	Code42/ Customer[1]	Customer	Customer
Is a BAA applicable?	Yes	Yes	N/A[2]	Yes	Yes	Yes
Will Code42 sign a BAA?	Yes	Yes	N/A[2]	Yes	Yes	Yes

1. In any instance where Code42 may have access to encryption keys, additional safeguards have been implemented.
2. A BAA is not applicable as Code42 will does not store/host any customer data or encryption keys.

FOR MORE INFORMATION: CODE42.COM/CONTACT

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM