CODE42

TECH OVERVIEW | COMPLIANCE

HOW CODE42 HELPS ORGANIZATIONS MAINTAIN HIPAA COMPLIANCE

Code42 endpoint data protection solutions (Incydr and CrashPlan) support customer compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule) requirements, giving organizations the critical data risk detection and response capabilities as well as data preservation capabilities needed for handling sensitive health information. In addition, Code42 provides a powerful data protection foundation that contributes to a long-term HIPAA compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

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 endpoint data protection solutions 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 Code42s endpoint data protection solutions 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’s HIPAA Compliance Support Page.

How Code42 Gives You Control of Your Data

Code42 endpoint solutions deliver several key functionalities that play a vital role in supporting HIPAA compliance:

1. **Secure 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 by automatically encrypting all endpoint data no matter where it lives or moves. Code42 Incydr gives you visibility to data exfiltration across a variety of vectors and provides protection against insider risk. This is the starting point of a comprehensive data security and data control strategy that supports HIPAA compliance.

2. **Maintain storage where you need it.** Code42 gives you the ability to choose where your data resides—and delivers the flexibility to choose from specific data centers globally. With the agile Code42 cloud platform, customers can elect to keep data at specific storage locations around the world, while still gaining the advantages and efficiencies of the cloud.
3. **Maintain complete data security.** Unlike other technology providers, Code42 doesn't have to deploy a specialized solution for customers that are subject to HIPAA. 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, utilizing FIPS 140-2 validated modules.
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 monitoring all endpoint data, Code42 delivers comprehensive visibility of your organization's most sensitive and valuable data.

   See how your employees move data across vectors— including web browser uploads, cloud sync activity, file sharing, Airdrop, and use of removable media. Know if and when users move sensitive health information outside your boundaries, so you can take action quickly to mitigate non-compliance and avoid potentially associated penalties and other losses, including reputational damage. Leverage this powerful data visibility to enable a proactive and intelligent approach to data security and protection. Establish baselines of normal individual user behavior and detect deviations or unusual activity. In short, spot anomalies sooner. Take action faster.

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (WP2010209)