

# How Code42 Helps Companies Meet Their Compliance Requirements

Nearly every organization today has legal, regulatory or compliance requirements they must meet to be viable in their industry. Code42 takes active measures to ensure all Code42 customer data is secure and that all deployments meet the most stringent security, compliance and operational requirements mandated by our customers.

Using Code42 in your environment may assist you in complying with relevant regulatory and security requirements. By deploying Code42 on your endpoints, you are able to address a variety of security controls across a number of security control frameworks.

Below is a list of some common security frameworks implemented across industries today and some of the key controls that can be addressed by Code42.

## Code42 Compliance Table:

Security Framework	Code42 Product Feature						
	Insider Threat	Encryption	Asset Management	Malware Protection	Audit/Logging	Backup	Incident Management
NIST 800-53	AC-21(2), AU-6(9), AU-13, CA-7, CP-9, IR-4(6), IR-4(7), PM-12, SC-30(4), SI-4, SI-4(19), SI-4(21)	SC-8, SC-28	AC-20(2)	SI-3	AU-2, AU-3, AU-3(1), AU-6, AU-12, AU-14	CP-6(1), CP-9, SC-28	IR-4(4), IR-9, CA-2(2)
NIST 800-171 (and DFARS)		3.13.8, 3.13.16	3.1.21	3.14.2	3.3.1, 3.3.2	3.8.9, 3.13.16	3.3.1
ISO 27001		A.10.1.1	A.8.3.1	A.12.2.1	A.12.4.1	A.12.3.1, A.17.2.1	A.16.1.2, A.16.1.7
HIPAA Security Rule		164.312(e)(2)(ii)	164.310(d)(1)		164.308(a)(1)(ii)(D)	164.308(a)(7)(ii)(A), 164.310(d)(2)(iv)	164.308(a)(6)(ii)
PCI DSS	12.10.5	3.5, 4.1		5.1, 5.4	10.3, 10.5, 10.7		

Don't see a regulation that impacts you? Reach out to your Code42 contact for additional regulations or compliance information.



## Code42 Key Compliance Features:

While security regulations may differ in scope and complexity, they all build off of basic information security best practices. It's in these foundational controls that Code42 provides the greatest support in reaching your compliance obligations:

### Insider Threat Protection

- Detect when users move files to removable media, web browsers/ applications and cloud sync folders
- Identify files that are shared externally via corporate OneDrive, Google Drive and Box accounts
- Define alert criteria based on user, data exfiltration vector and file count or size
- Monitor and alert on use of removable media and portable storage devices

### Detection and Response to Incidents

- Security teams can review event activity in seconds, even when user devices are offline
- All file activity is automatically indexed and made searchable to reduce the time it takes to detect and respond to insider threats

### File Preservation

- Code42 protects the confidentiality, integrity and availability of your data by preserving exact copies of files that can be restored
- Files and their respective metadata are encrypted before secure transmission to storage servers, where data remains encrypted at rest

### Malware Protection

- Code42 provides malicious code protection mechanisms on user endpoints
- Endpoint file preservation provides point-in-time recovery from malicious software

### Encryption

- Code42 protects the confidentiality and integrity of transmitted information and information at rest
- Communications between the Code42 endpoint app and the storage servers are encrypted using AES 256-bit encryption
- Files and their respective metadata are AES 256-bit encrypted in the endpoint app and remain encrypted in storage servers

### Audit/Logging

- Code42 allows organizations to log file activity on user endpoints
- Code42 generates audit records with the following event information:
  - Type
  - Date/time
  - Location
  - Source
  - Outcome
  - File involved
  - Identity of any individuals or subjects associated with the event

### Incident Management

- Code42 provides file activity and the ability to view endpoint files to support after-the-fact investigations of security incidents
- Code42 allows for detailed analysis of user file movement activity on a device

Code42 is committed to helping organizations reach their compliance obligations. If you have additional questions about how Code42 can assist with your organizational compliance needs, please contact your Code42 representative today.



CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | [CODE42.COM](https://code42.com)

Code42 is the leader in insider risk detection, investigation 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 from insider threats while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider threat 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. For more information, visit [code42.com](https://code42.com), read [Code42's blog](#) or follow the company on [Twitter](#). © 2020

OV2006196