How **Acronis** Cyber Protect enables health care organizations to maintain HIPAA compliance

Many industries rely heavily on automation for real-time production processes, including the automotive, energy, power, pharmaceutical and logistics sectors. Much of that automation technology is controlled, configured and monitored by PCs running Windows or Linux that fall under the rubric of operational technology (OT), industrial control systems (ICS) and cyber-physical infrastructure. Common OT applications include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), human-machine interfaces (HMI), and operational historian systems that capture real-time process data.

Compliance with the strict standards imposed by the Health Insurance Portability and Accountability Act (HIPAA) continues to be a major challenge for health care organizations.

HIPAA requires organizations that deal with health care-related data to comply with strict standards of data privacy and security. Ensuring the confidentiality, integrity and availability of patient data is not only a legal obligation, but also a critical aspect of providing high-quality patient care.

Specifically, disaster recovery and data security present major challenges to organization grappling with HIPAA compliance. Acronis Cyber Protect offers a comprehensive solution that addresses those challenges, providing robust data protection and disaster recovery capabilities that are fully compliant with HIPAA regulations.

Disaster recovery and data security present major challenges to organizations grappling with HIPAA compliance

HIPAA COMPLIANCE

Challenges in maintaining HIPAA compliance

One of the major issues organizations face in complying with HIPAA is data security. Health care organizations need to implement strong encryption and access controls to ensure data remains confidential and secure.

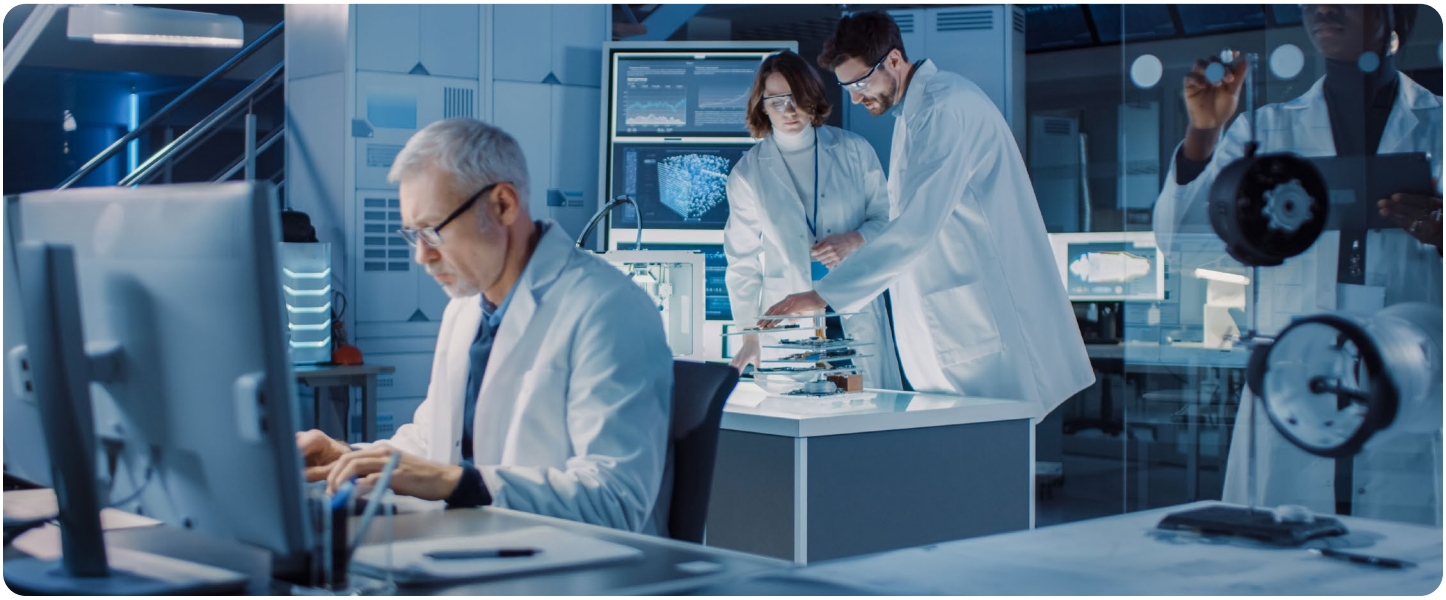
Maintaining data integrity and availability are challenges, too. Any data corruption or loss can have severe consequences, including legal and financial penalties. Health care organization need to be sure that patient data is always accessible so that they can stay compliant and provide timely and effective health care services.

Strict regulatory compliance and auditing requirements, including maintaining detailed logs and records of data access and management, are another difficult issue organizations face.

How Acronis Cyber Protect empowers organizations to meet HIPAA requirements

Many health care organizations are hesitant to store data in the cloud due to concerns about compliance and privacy. Acronis Cyber Protect has them covered with encrypted, on-premises functionality for cybersecurity and backup and recovery.

- **Advanced encryption:** Uses industry-leading encryption to protect patient data both in transit and at rest. This practice ensures that critical information remains secure and compliant with HIPAA requirements, whether it's stored locally or in the cloud. Ultra-strong encryption helps prevent unauthorized access and data breaches, maintaining the confidentiality of patient information.
- **Seamless data management:** Provides comprehensive data management capabilities, including automated backups, one-click recovery and granular data restoration. Those functions help health care organizations maintain data integrity and availability, ensure that data is consistently protected and enable efficient, rapid restoration.
- **Comprehensive security features:** Delivers advanced malware and ransomware protection, and AI-driven threat detection and response. Together, they ensure that potential security threats are identified and mitigated in real time, prevent data breaches and ensure protection of patient information.
- **HIPAA-compliant disaster recovery:** Features such as secure data replication, failover and failback, ensuring that health care organizations can quickly recover from disasters without compromising patient data.
- **Detailed auditing and reporting:** Provides detailed logs and reports, including records of data access, backup activities and security events. Ensuring transparency and accountability, these reporting features help organizations maintain a clear and detailed audit trail.



Acronis Cyber Protect provides the capabilities necessary for HIPAA compliance

The features in Acronis Cyber Protect line up with a list of 10 HIPAA requirements, including:

1. Requirement 164.312(a)(2)(iv)
AES-256 encryption — Ensures robust encryption to safeguard the confidentiality and integrity of electronic protected health information (ePHI).

2. Requirement 164.308(a)(7)(ii)(A-B)
Immutable backups, off-site storage, geo-redundancy — Uses encryption for immutable backups, cloud-based, off-site storage and geo-redundancy to ensure data availability and resilience.

3. Requirement 164.312(a)(1)
Role-based access control — Enables administrators to implement technical policies and procedures to restrict access to ePHI to authorized individuals only.

4. Requirement 164.312(b)
Audit logging and reporting — Delivers logs and reports that ensure transparency and accountability.

5. Requirement 164.312(d)
Multifactor authentication (MFA) — Features multifactor authentication (MFA) through centralized access control systems, using secure mechanisms and authentication protocols such as LDAP, Kerberos and SSH certificates, zero trust access, unique user IDs, strong passwords and two-factor authentication mechanisms.

6. Requirement 164.310(d)(1)
Data loss prevention (DLP) — Includes policies and procedures governing the removal, reuse and disposal of electronic media containing PHI. Backup and recovery, as well as disaster recovery, enable organizations to prevent data loss.

7. Requirement 164.308(a)(7)(ii)(B)
Continuous data protection and disaster recovery (CDP and DR) — Ensures continuous data protection and disaster recovery by providing seamless management, rapid data recovery and unified protection, including Acronis Instant Restore and support for recovery to any platform.

8. Requirement 164.308(a)(1)(ii)(A)
Vulnerability assessment and patch management — Performs vulnerability scans of internal and data center infrastructure, in accordance with the Annual Program of Vulnerability Scans, to ensure information security controls and safeguards. With automated patch management, administrators can roll back to previous versions of files and applications in case a patch causes an error.

9. Requirement 164.308(a)(5)(ii)(B)
Endpoint detection and response (EDR) — Covering all five functions of the NIST Cybersecurity Framework, Acronis EDR continuously monitors, detects and enables responses to potentially threatening activity.

10. Requirement 164.312(e)(2)(ii)
FIPS 140-2 encryption — Acronis Cyber Protect includes encryption mechanisms that comply with HIPAA standards to protect ePHI transmitted over electronic communication networks.

Acronis Cyber Protect addresses key pain points for organizations with HIPAA responsibilities

With Acronis Cyber Protect, health care organizations can confidently meet and maintain HIPAA compliance. The solution's advanced encryption, comprehensive data management and robust security features ensure that patient data remains secure and accessible. Additionally, HIPAA-compliant disaster recovery capabilities provide a reliable and efficient way to recover from disasters, ensuring that health care organizations can continue to provide high-quality patient care without the burden of compliance concerns.

Learn more about Acronis Cyber Protect READ

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection and endpoint management for educational institutions, managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity.

Acronis offers the most comprehensive security solution on the market with its unique ability to meet the needs of diverse and distributed IT environments. A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers and over 750,000 businesses and educational institutions.

Acronis

Learn more at
www.acronis.com