Acronis

WHITE PAPER

Comply with HIPAA Using **Acronis** Solutions

Table of contents

Introduction

Today's cloud technologies offer a wide range of solutions that medical organizations can use to easily and securely process protected health information (PHI). Knowing that these tools meet the strict regulatory requirements of the healthcare industry is not as easy, though.

When it comes to protecting the security and privacy of PHI, the two primary regulations are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). Together, they establish a fundamental set of requirements that can be summed up in three main rules[1]:

- **Privacy Rule**
- **Security Rule**
- **Breach Notification Rule**

While compliance is required, there is no official, legally recognized certification process or accreditation for HIPAA. As a result, healthcare providers must not only evaluate a possible IT solution based on the benefits it offers, but also whether it meets regulatory requirements. They also need to get that analysis right since HIPAA compliance is a shared responsibility of their organization and the cloud vendor they choose.

In response, Acronis established and maintains a HIPAA-HITECH security and compliance program for services offered as part of Acronis Cyber Protect Cloud. Designed to ease customer compliance concerns, the program ensures our solutions uphold the strict security and privacy standards demanded by HIPAA-HITECH.

This document has been prepared to help security, compliance, and IT officials understand the measures Acronis takes in order to comply with these regulations.

NOTE: Acronis Cyber Protect Cloud is a platform that supports multiple services (or products). Therefore, individual Acronis service functions and HIPAA compliance status can vary depending on the service and data center. Please talk to your account manager to clarify the compliance status of particular services and data centers.

NOTE: This document and any other related documentation on compliance produced by Acronis does not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations under HIPAA, as well as for using Acronis Cyber Protect Cloud services in an appropriate manner under HIPAA requirements. All specific service functions can be found via https://www.acronis.com/en-us/support/documentation/

1 Additional information on HIPAA and HITECH can be found at https://www.hhs.gov

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect an individual's medical records and other personal health information (PHI). It applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.

The Privacy Rule requires appropriate safeguards to protect the privacy of PHI, and sets limits and conditions on the uses and disclosures of this information when patient authorization has not been obtained. The rule also grants patients' rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

Under HITECH, the Privacy Rule obligations extend to "Business Associates." This term generally refers to contractors (e.g. data protection vendors like Acronis) that are delegated by an organization (the "Covered Entity") to orchestrate some or all of its obligations under the rule.

This relationship and the role of the associate should be stipulated in a Business Associate Agreement.

A Business Associate Agreement establishes responsibilities within the scope of HIPAA requirements. It also defines any obligations among the two parties regarding PHI processing and protection within the services utilized.

Acronis took care to develop a Business Associate Agreement for Acronis Cyber Protect Cloud solutions, taking into account specific capabilities of Acronis Cyber Protect Cloud services and Acronis' role in the processing and protection of PHI.

> **NOTE:** Acronis' Business Associate Agreement is available upon request. Please contact an account manager.

HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect an individual's electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity (expanded to include Business Associates by HITECH).

The HIPAA Security Rule establishes national standards to protect an individual's electronic personal health information (ePHI). This means information that is created, received, used, or maintained by a Covered Entity (or Business Associate, per HITECH) requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI.

All requirements of the HIPAA Security Rule are divided into three parts:

- **Administrative Safeguards**
- **Physical Safeguards**
- **Technical Safeguards**

ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards are in place to protect electronic health information and manage the conduct of employees accordingly. Safeguards include administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures.

With respect to the Administrative Safeguards, Acronis developed and maintains an information security management system based on the broadly accepted international security standard ISO 27001:2013. This system is certified by the British Standard Institution (BSI), the world's first national standards body.

Acronis' system manages policies and procedures that define and regulate required aspects of HIPAA as follows:

Security Management Processes

Acronis maintains the information security management system so that the information security controls and safeguards are implemented based on a risk analysis that examines relevant threats, while ensuring customer data is valued as the most critical asset.

Acronis employees are also held to these standards. Should violations be found among any involved parties, sanctions are issued per local law.

Acronis' Network Operations Center (NOC) constantly monitors Acronis Cyber Protect Cloud services to detect issues, identify the root cause, and contact the appropriate internal incident response team to triage and resolve the technology incident per the established procedures.

> **NOTE:** Acronis does not control how the customer uses cloud services for PHI processing, or the customer's security management process. Customers should conduct their own risk analysis, implement a risk management plan and a sanctions policy, and conduct an information system activity review. As part of the security management process, customers should consider how Acronis Cyber Protect Cloud services or specific Acronis products fit within its policies and procedures to prevent, detect, contain, and correct security violations.

Assigned Security Responsibilities

Acronis' dedicated Security team develops and implements internal security policies and procedures. The Chief Information Security Officer (CISO) is responsible for maintaining the security posture of Acronis.

Workforce Security and Information Access Management

All Acronis personnel are obligated to comply with Acronis' confidentiality, business ethics, and code of conduct policies. Acronis pays special attention to personnel selection by conducting appropriate background checks on candidates for employment, in accordance with applicable local laws, statutory regulations, and ethics. Every Acronis employee is required to sign a Non-Disclosure Agreement (NDA).

Authorization and termination of an Acronis employee's access to any information resources are carried out in accordance with internal procedures. These standards consider a person's official duties and applies the principles of "Need to Know" and "Least Privileges."

> **NOTE:** Acronis does not control how the customer uses cloud services for PHI processing. Due to product specifications, Acronis cannot recognize and separate different types of data. Rather, all customer data is classified as the highest critical asset,
> in accordance with Acronis' internal data classification policy.
>
> **NOTE:** Acronis employees do not access customer data within data centers. Customer and management environments are logically isolated.

Security Awareness and Training

All Acronis employees receive awareness education and training regarding information security, privacy protection, and data processing, as is appropriate relative to their job functions and assigned roles.

> **NOTE:** Customers should maintain their own security awareness and training program, including information about how to use and configure Acronis Cyber Protect Cloud services to comply with their internal policies and HIPAA requirements (e.g. how to monitor login attempts and other logs generated by the systems).

Security Incident Procedures

Acronis' Network Operations Center (NOC) leads incident identification and response, identifies the root cause of any problem, and contacts the appropriate internal incident response team.

Acronis has developed several different escalation paths, based on the type of incident and its severity. Global or high-severity level incidents are escalated directly to Acronis' executive staff. Acronis' incident management culture is based on global best practices.

There are seven stages for handling every incident:

1. **Preparation.** Acronis educates users and IT staff after every incident and new implementation, and trains them to respond to incidents quickly and correctly.
2. **Identification.** The team is activated and decides whether an event is, in fact, an incident. (Information about the incident can come from Acronis' monitoring system or communication via different teams and customers.)
3. **Containment.** The team determines the impact, problem coverage, and the affected systems and customers.
4. **Eradication.** The team investigates to discover the origin of the incident and the root cause of the problem, and then begins the triage process.
5. **Recovery.** The team monitors every environment for any sign of weakness or recurrence.
6. **Lessons learned.** The team analyzes the incident and how it was handled, making recommendations to prevent a recurrence and plan for the next incident response.
7. **Notification.** Internal and external communications ensure all teams and customers understand the impact and resolution steps, and are updated every hour during an incident, or at every significant state of change. Notifications are critical and accompany all stages of incident triage.

Contingency Plans

Many potential disruptive threats can occur at any time and impact business operations at any location. Acronis considers a wide range of potential threats as part of the risk and business-impact analysis at all Acronis locations and acts to mitigate such threats.

Acronis maintains a Business Continuity and Disaster Recovery (BCDR) Program that addresses its critical processes and technology at all of its data centers. Acronis periodically conducts tests and updates of its internal BCDR Plans in order to ensure an adequate reaction and availability of services should disruptive events occur.

Acronis has established partnerships that run numerous, global, co-located data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power, and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data center locations to reduce or eliminate the probability of the most typical disruptive events.

Evaluations

Acronis continually monitors and periodically evaluates applied controls and processes against established requirements of information security and data processing. This procedure ensures the proper implementation of the information security and compliance program. In turn, Acronis can adequately measure the degree of program implementation as well as detect and respond to new information security risks in a timely manner.

In accordance with Acronis' internal policies and procedures, the following evaluation activities are provided:

- **Penetration tests.** Performed by a third party on an annual basis.
- **Vulnerability assessment.** Acronis performs vulnerability scans of internal and data center infrastructure, in accordance with the Annual Program of Vulnerability Scans.
- **External and internal audits.** Acronis regularly checks its processes, by conducting internal and external audits.

Business Associate Agreement and Other Arrangements

The Business Associate Agreement (BAA) establishes responsibilities within the scope of HIPAA requirements and defines obligations of the Covered Entity and Business Associate, regarding PHI processing and protection within the Acronis Cyber Protect Cloud services.

Acronis took care to develop the BAA, taking into consideration the specifics of Acronis Cyber Protect Cloud services and Acronis' role in the processing and protection of PHI.

The Acronis BAA is available upon request. Please contact an account manager.

PHYSICAL SAFEGUARDS

Physical Safeguards are a set of rules and guidelines that focus on physical access to PHI.

Acronis hosts customer data within trusted data centers, which employ the highest standards of physical security to restrict unauthorized physical access and maintaindata safety.

There are three standard requirements for HIPAA Physical Safeguards as follows:

Facility Access Controls

Only authorized personnel have access to data centers. Data centers have strict access management, control protocols (access control cards or biometric access control systems), and surveillance cameras (CCTV).

All equipment is located in special cages, which are also locked and monitored.

Workstation Use and Security

Although customer data does not leave the data center and Acronis employees do not access customer data, Acronis applies procedures and configuration standards to employees' workstations. This approach establishes acceptable use of those workstations (e.g. workstations accounting, full HDD encryption, auto lock, antivirus, clear-screen policy, taking off-site control, etc.).

Device and Media Controls

Acronis uses a software-defined storage solution, which utilizes a proprietary erasure-coding algorithm, and which securely removes customer data. In the case Acronis Cyber Infrastructure drives and equipment are broken, switched out for repair, or decommissioned, Acronis takes measures to erase data from a disk and remove residual data from the internal memory of the equipment, according to NIST SP 800-88rev1.

In the event that it is not possible to erase (delete) such information, equipment is physically destroyed in such a way that it's impossible to read (restore) such data.

TECHNICAL SAFEGUARDS

The Technical Safeguards focus on the technologies (software and hardware) that protect and control access to PHI. The standards of the Technical Safeguards do not require the use of any specific vendor.

There are five standards under Technical Safeguards as follows:

Access Control

Acronis maintains an enterprise-wide access control policy that restricts access to information resources and data, in accordance with official duties. Access provisioning is based on the principles of "Need to Know" and "Least Privileges."

Internal access control procedures detect and prevent unauthorized access to Acronis systems and information resources. When providing access, Acronis uses centralized access control systems with secure mechanisms and authentication protocols (e.g. LDAP, Kerberos, and SSH certificates, zero trust access), unique user IDs, strong passwords, two-factor authentication mechanisms, automatic logoff, and limited control access lists minimizing the likelihood of unauthorized access.

Acronis products also provide access control mechanisms such as unique user IDs, password complexity and two-factor authentication, automatic logoff, session termination, and encryption. Some products can be integrated with Active Directory and enforce a customer's policies.

Acronis Cyber Protect Cloud services enforce in-transit and at-rest data encryption by default, with reliable cryptographic algorithms and protocols (e.g. TLS, SSH, IPSec, AES, etc.), though these HIPAA requirements are only deemed "addressable."

In addition, some products allow data encryption by using a customer's keys, with a length up to 256 bit.

Audit Controls

Acronis uses procedural, software, and hardware mechanisms to audit activities at the backend of Acronis Cyber Protect Cloud services.

Acronis Cyber Protect Cloud services can provide a chronological record of the following events:

- Operations performed by users in the management portal or service
- System messages (e.g. warnings, errors, etc.)

The log shows events in the tenant in which customers are currently operating and its child tenants.

The default retention period of the logs is not less than 180 days.

> **NOTE:** Depending on the service, the retention period can vary and be configured by the customer in accordance with their internal policies and legal obligations. For additional information, visit https://www.acronis.com/en-us/support/documentation/.

Integrity

Acronis products provide mechanisms that protect ePHI from improper alteration or destruction. These mechanisms include access control, reliable networks protocols, encryption, hashing, and validation, which work by defaultor can be configured by the customer by using specific Acronis Cyber Protect Cloud services.

Acronis Cyber Infrastructure is a software-defined storage where all customer data is kept and which utilizes a proprietary erasure-coding algorithm to enhance reliability and protection against failures. It includes scalable and efficient self-healing mechanisms to minimize data risks. In addition, Acronis Cyber Infrastructure utilizes a fully redundant architecture to safeguard data integrity for every customer.

Authentication

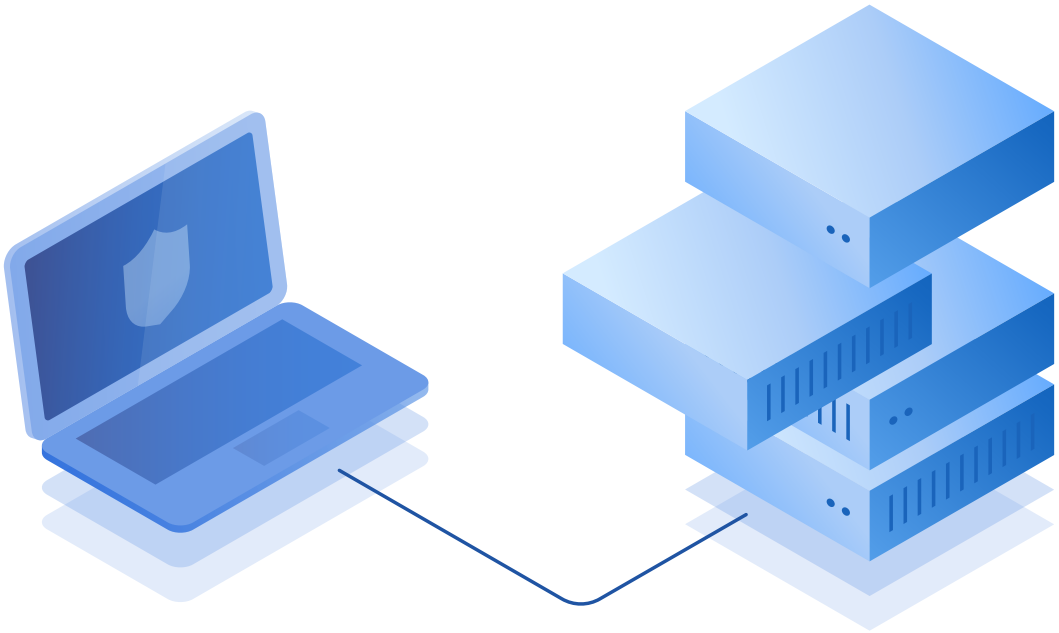
Acronis maintains an enterprise-wide access control policy to restrict access to information resources and data, in accordance with official duties. Access provisioning is based on the principles of "Need to Know" and "Least Privileges."

Internal access control procedures detect and prevent unauthorized access to Acronis systems and information resources. When providing access, Acronis uses centralized access control systems with secure mechanisms and authentication protocols (e.g. LDAP, Kerberos, and SSH certificates, zero trust access), unique user IDs, strong passwords, two-factor authentication mechanisms, automatic logoff, and limited control access lists, minimizing the likelihood of unauthorized access.

Acronis products also provide access control mechanisms, such as unique user IDs, password complexity and two-factor authentication, automatic logoff, session termination, and encryption. Some products can be integrated with Active Directory to help enforce customer policies.

Transmission Security

To protect information while in-transit over electronic communications networks, Acronis Cyber Protect Cloud services use reliable networks protocols, which ensure ordered and error-checked delivery, together with cryptographic protocols. These ensure the integrity, authenticity, and confidentiality of transmitted data (e.g. TLS, SSH, etc.).



HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires HIPAA-covered entities and their Business Associates to notify impacted parties following a breach of unsecured protected health information (PHI).

In the event a breach affects more than 500 patients, the media and public must also be notified.

Covered Entities and Business Associates, as applicable, have the burden of demonstrating that all required notifications have been provided, or that a use or disclosure of unsecured PHI did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a Covered Entity (or Business Associate) should maintain documentation that all required notifications were made, or alternatively, provide documentation stating notification was not required.

Exceptions include:

- A risk assessment demonstrating a low probability that PHI has been compromised by the impermissible use or disclosure.
- The application of any other exceptions to the definition of "breach."

Acronis maintains a Data Breach Response and Notification Procedure, which considers the HIPAA requirements and describes how Acronis must act in the case of a data breach (e.g. roles, priority, escalation, timing, etc.).

NOTE: As Covered Entities, customers must comply with certain administrative requirements with respect to breach notification. For example, Covered Entities must have written policies and procedures in place regarding breach notification, train employees on these policies and procedures, and develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Acronis

Learn more at
www.acronis.com