blancco

How Does Blancco Help Organizations Achieve HIPAA Compliance?

The Health Insurance Portability and Accountability Act (HIPAA) is a 1996 U.S. federal law that regulates the use and disclosure of protected health information (PHI), and includes requirements for data disposal.

HIPAA is applicable to organizations that offer health plans, to health care clearinghouses and to any health care providers that transmit health information in electronic form. It is also applicable to entities that create, receive, maintain, or transmit any PHI on behalf of a covered entity or another business associate acting as a subcontractor. This includes government-owned institutions.

HIPAA and Data Sanitization

While HIPAA doesn't put specific data sanitization rules in place, it does speak about the need to dispose of data that is no longer required to meet HIPAA compliance needs. It's up to your organization to establish secure data removal policies to avoid fines for noncompliance.

In 2013, the HIPAA Omnibus Rule was put in place. This rule increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident.

Complying with HIPAA

Adhering to HIPAA Title II is what most organizations mean when they refer to HIPAA compliance. Also known as the Administrative Simplification provisions, Title II includes the following HIPAA compliance requirements:

- **National Provider Identifier Standard.** All healthcare entities must have a unique, 10-digit national provider identifier number, or NPI.
- **Transactions and Code Sets Standards.** A standardized mechanism for electronic data interchange (EDI) for processing insurance claims.
- **HIPAA Privacy Rule.** Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule establishes national standards to protect patient health information.

- **HIPAA Security Rule:** The Security Standards for the Protection of Electronic Protected Health Information sets standards for patient data security.
- **HIPAA Breach Notification Rule:** Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
- **HIPAA Enforcement Rule.** This rule establishes guidelines for investigations into HIPAA compliance violations.

Specifically, Blancco helps organizations comply with the HIPAA Privacy Rule and the HIPAA Security Rule.

The HIPAA Privacy Rule

The HIPAA Privacy Rule concerns "national standards to protect individuals' medical records and other personal health information."

This Rule requires that organizations implement safeguards to protect patient data. Blancco's suite of data erasure solutions enable organizations to meet HIPPA compliance by erasing electronic records when they're no longer needed.

For example, Blancco File Eraser allows organizations to go beyond file shredding with secure erasure of sensitive files and folders with system integrations and rules automation. This cost-effective solution ensures data is made unrecoverable, fully satisfying the HIPAA Privacy Rule requirement when data no longer fulfills a business or retention need.

HIPAA Security Rule

The HIPAA Security Rule protects a subset of electronic information covered by the HIPAA Privacy Rule. The Security Rule refers to this information as "electronic protected health information" (e-PHI).

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

The following chart shows how Blancco helps address HIPAA Security Rule requirements.

blancco

RULE	DESCRIPTION	HOW BLANCCO HELPS
HIPAA Security Rule, Subpart C	**§ 164.306 Security standards: General rules.** **(B) Risk management** (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). **(D) Information system activity review** (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.	Blancco data erasure solutions allow organizations to securely and permanently erase data across its lifecycle to meet and exceed HIPAA requirements. Through programmatic processes that automate data erasure per policy and requirement, Blancco solutions ensure that all ePHI is erased when it no longer needs to be stored, maintained, or made available to a covered entity or business associate. This allows you to protect the integrity and confidentiality of ePHI so you can prove compliance with 164.306(a). Blancco data erasure solutions also reduce the attack surface by minimizing the quantity of data available in the event of a data breach. Blancco Management Portal, as well as its predecessor, Blancco Management Console, allows organizations to manage data erasure across all IT assets within a single program for consolidated reporting, producing a 100-percent certified audit trail.
HIPAA Security Rule, Subpart C	**§ 164.308 Administrative safeguards.** **(1)(i) Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.	Implementing a comprehensive data erasure policy across the data lifecycle for active and end-of-life assets is best practice to maximize data security and prevent security violations. Blancco data erasure solutions can easily be added as another layer of security to your existing security management process.
HIPAA Security Rule, Subpart C	**§ 164.314 Organizational requirements.** **(a)(2)(i) Business associate contracts.** The contract between a covered entity and a business associate must provide that the business associate will— (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart.	Integrating data erasure best practices into business associate contracts allows organizations to remove data when it's no longer needed or required for HIPAA compliance. This helps protect sensitive information against exposure in the event of a data breach.

blancco

RULE	DESCRIPTION	HOW BLANCCO HELPS
HIPAA Security Rule, Subpart C	**§ 164.314 Organizational requirements.** (b)(2)(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	Blancco data erasure solutions should be implemented beyond the contract level; they should be implemented across the information management lifecycle, when it's created, received, maintained, or transmitted.
HIPAA Security Rule, Subpart C	**§ 164.316 Policies and procedures** **Time limit (Required)**. Retain the documentation required by paragraph (b) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	After HIPAA time limits (retention periods) have expired, data should be disposed of securely. Implement automated data erasure policies to erase data that's no longer needed.
HIPAA Security Rule, Subpart C	**§ 164.310 Physical Safeguards** **(d)(2)(i) Disposal required:** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. **(d)(2)(ii) Media re-use:** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Blancco data erasure solutions ease compliance by allowing policy-based erasure for active files. This enables data to be deleted based on retention or file data, level of confidentiality, or other specified characteristic in order to meet compliance. This can be implemented locally on individual PCs and laptops or anywhere across an organization's infrastructure, including within virtual machines and cloud networks. Blancco Drive Eraser and other erasure solutions ensure that data residing on embedded or loose hardware is completely overwritten and rendered inaccessible, protecting against data privacy violations and enabling safe and secure reuse.
HIPAA Security Rule, Subpart D	**§ 164.504 Uses and disclosures: Organizational requirements.** **(ii) Provide that the business associate will:** At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.	Data erasure solutions can destroy data at termination of contract, including data on laptops, computers, HDDs, SSDs, removable media, and virtual machines. A certificate of erasure is provided for every erasure that occurs, producing a 100- percent tamper-proof audit trail.

RULE	DESCRIPTION	HOW BLANCCO HELPS
HIPAA Security Rule, Subpart D	**§ 164.504 Uses and disclosures: Organizational requirements.** (l) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction.	Blancco data erasure solutions allow organizations to automate erasure on an ongoing basis, while Blancco Management Portal, as well as its predecessor, Blancco Management Console, lets organizations keep track of all certificates of destruction to prove compliance and pass audits.

Protect ePHI Patient Information with Blancco Data Erasure Solutions

Blancco's intuitive and flexible data erasure software allows highly regulated organizations to easily automate their data destruction needs to improve security, privacy, and compliance.

With Blancco solutions, your organization can permanently erase ePHI at the right time—in a active or inactive environments—to protect your employees and your patients.

Complete with audit capabilities, Blancco Management Portal, as well as its predecessor, Blancco Management Console provides detailed reporting that includes everything needed for HIPAA compliance, including security information, user data, serial numbers, exact times of erasure, and more.

To further align to your internal requirements, administrators can add custom fields to capture vital information relevant to your process, allowing for centralized control and reporting of all data erasure activities across every IT asset.

Why Blancco?

For more than 25 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as HIPAA. We equip heavily regulated industries with the tools they need to stay compliant with these regulations, offering data erasure solutions that satisfy (and often exceed) regulatory requirements.

Securely and efficiently erase no-longer-needed PHI.
Request your **free data erasure trial** today.