How Does Blancco Help Organizations Achieve HIPAA Compliance?

The Health Insurance Portability and Accountability Act (HIPAA) is a 1996 Federal law that restricts access to individuals' private medical information. HIPAA is applicable to organizations that offer health plans, health care clearinghouses and any health care providers that transmit health information in electronic form. 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 put secure data removal policies in place 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 Enforcement Rule**. This rule establishes guidelines for investigations into HIPAA compliance violations.

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

HIPAA Privacy Rule

The HIPAA Privacy Rule concerns "national standards to protect individuals' medical records and other personal health information". [1] This Rule requires that organizations implement safeguards to protect patient data. Blancco's suite of Data Eraser solutions are essential to enable organizations satisfy this requirement by erasing electronic records when they're no longer needed to meet HIPPA compliance. For example, Blancco File Eraser allows organizations to go beyond file shredding with secure erasure of sensitive files/folders with integration and automation of rules. This cost-effective solution ensures the data are made unrecoverable to fully satisfy this requirement.

1 https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

blancco

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. See the chart below to find out how Blancco can help address the HIPAA Security Rules.

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 Eraser 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 associated. 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 reduces the attack surface by minimizing the quantity of data available in the event of a data breach. Blancco Management Console allows organizations to manage data erasure across all IT assets within a single program for consolidated reporting, producing a 100% 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 Eraser 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.** (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.

Continued...

Rule	Description	How Blancco Helps
HIPAA Security Rule Subpart C	**§ 164.314 Organizational requirements.** (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.	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** (i) Time limit (Required). Retain the documentation required by paragraph (b) (1) 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 D	**§ 164.504 Uses and disclosures: Organizational requirements.** (ii) Provide that the business associate will: (I) 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% tamper-proof audit trail.
HIPAA Security Rule Subpart D	**§ 164.504 Uses and disclosures: Organizational requirements.** (I) 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 Console lets organizations keep track of all their certificates of destruction to prove compliance and pass their audits.

Continued...

blancco

Protect Patient Information with Blancco Data Eraser 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 tamper-proof environment – to protect your employees and your patients.

Complete with audit capabilities, 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 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as HIPAA. We support the need for heavily-regulated industries to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Contact us today for additional information about how we can help you pass your next data security and compliance audit.