HIPAA Data Sanitization Requirements

While HIPAA does not 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 is up to your organization to put secure data removal policies in place to avoid fines for noncompliance and to eliminate data in totality to avoid the risk of unauthorized data recovery. 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.

HIPAA, Security rules, and Disposal of Protected Health Information:

“The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(C). This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.”

Complying with HIPAA

Adhering to HIPAA Title II is what most organizations mean when they refer to HIPAA compliance. Also known as the administrative Simplifications 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(NPI).

Transactions and Code Sets Standards. A standardized mechanism for electronic data interchange (EDI) for processing insurance claims.

HIPAA Enforcement Rule. This rule establishes guidelines for investigations into HIPAA compliance violations.

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.

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

HIPAA Privacy Rule

Officially known as the Standards for Privacy of Individually Identifiable Health Information. The HIPAA Privacy Rule concerns “national standards to protect individuals’ medical records and other personal health information”. This rule requires organizations to implement safeguards to protect patient data.

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” (ePHI). The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards for protecting ePHI.

What is Data Sanitization?

Practicing effective data sanitization should be part of an overall security strategy for retiring or reusing IT assets and eliminating protected health information so that the data stored on those devices are not at risk of falling into the wrong hands.

According to the International Data Sanitization Consortium, “Data Sanitization is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered. There are three methods to achieve data sanitization: physical destruction, cryptographic erasure, and data erasure.”

Although data destruction and data sanitization have similarities in their approach, they are not the same. Data destruction does not include verification or certification of successful destruction beyond forensic recovery. This means that the chosen data destruction method has not been proven to remove data in totality, whether that target data is a single file or an entire drive.

Visit www.clarabyte.com to read our eBook on Data Sanitization Best Practices

HIPAA SECURITY RULE - SUBPART C

SPECIFICATION	DATA SANITIZATION SIMPLIFICATION
§ 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.	Maintain an audit trail for erasure events.
§ 164.308 Administrative safeguards. **(1)(I) Standard:** Security management process. Implement policies and procedures to prevent, detect, contain and correct security violations.	Data sanitization should be implemented as part of a comprehensive security strategy.

§ 164.314 Organizational requirements - Implementation Specifications (Required). **(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.	Require that any business associate which has access to ePHI has data sanitization policies in place and utilizes the appropriate technologies.
§ 164.314 Organizational requirements - Requirements for group health plans - Implementation specifications (Required). **(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 sanitization should be applied to end-of-life and temporary health records to confirm complete removal.
§ 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 was last in effect, whichever is later.	Perform data sanitization on records that have met the end of their retention period, to limit liability. Produce a tamper-proof audit report to demonstrate compliance.

HIPAA SECURITY RULE - SUBPART D

SPECIFICATION	DATA SANITIZATION SIMPLIFICATION
§ 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.	Destroy all protected data with proper data sanitization techniques. Produce a tamper-proof audit report to demonstrate compliance.

§ 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 such as 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.	Destroy all protected data with proper data sanitization techniques. Produce a tamper-proof audit report to demonstrate compliance.

Protect Patient Information with Clarabyte's Data Destruction Solution

Clarabyte's intuitive and flexible data erasure software allows highly regulated organizations to easily automate their data sanitization processes to improve security, eliminate the risk of human error when processing devices, and to guarantee compliance with HIPAA. Clarabyte's proprietary algorithm offers data erasure for the entire spectrum of hard drives and solid-state drives, with verification of successful erasure, and tamper-proof reporting. This unmatched level of control over data removal provides assurance that no trace of target data remains on a device and compliance is guaranteed.

Click here to learn more about ClaraWipe Pro.

References:

https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

https://www.datasanitization.org/data-sanitization-regulations/