

HIPAA was established in 1996 to protect medical records by establishing transaction standards for the exchange of health information, security standards and privacy standards for the use and disclosure of individually identifiable health information.

To achieve compliance with HIPAA requirements, organizations must establish and enforce policies that safeguard the integrity and availability of confidential electronic information.

Sanctuary Helps Healthcare Organizations Comply with HIPAA for Endpoint Security

Sanctuary ensures electronic protected health information (ePHI) privacy by enforcing encryption when copied to removable media. Sanctuary also provides detailed audit information to prove HIPAA compliance. With Sanctuary, only authorized users can copy ePHI onto encrypted removable media with complete auditing of that action.

By employing a whitelist approach, Sanctuary is uniquely capable of enforcing application and device usage and control policies, which enables only authorized applications and devices to run or connect to a network, server, terminal services server, laptop, thin client or desktop – facilitating security and systems management, while providing necessary flexibility to the organization to easily enable the use of new/upgraded applications or devices.

Through policy-based control at the endpoints to monitor and control the inbound and outbound flow of ePHI to media and devices, Sanctuary complements organizations' HIPAA compliance strategy by implementing administrative, physical and technical safeguards around application and removable device use:

HIPAA Administrative Safeguards

HIPAA Requirement - **164.308(a)(1)(i)** – ***Security Management Process***

Implement policies and procedures to prevent, detect, contain and correct security violations.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enables organizations to define and enforce policies regarding authorized applications and removable devices. Any unwanted, unauthorized and/or malicious applications as well as any unwanted devices are denied by default.

HIPAA Requirement - **164.308(a)(1)(ii)(B)** - ***Risk Management***

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

How Sanctuary Addresses HIPAA Requirements

Sanctuary enforces policies regarding authorized applications and removable devices to reduce risks

and vulnerabilities.

HIPAA Requirement - 164.308(a)(1)(ii)(C) - [Sanction Policy](#)

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

[How Sanctuary Addresses HIPAA Requirements](#)

Sanctuary assures every workforce members' compliance with organizational endpoint security policies governing application and device control. Detailed auditing capabilities provide the capability to identify any workforce member who attempts to disregard security policies and procedures.

HIPAA Requirement - 164.308(a)(1)(ii)(D) - [Information System Activity Review](#)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

[How Sanctuary Addresses HIPAA Requirements](#)

Sanctuary logs any program and I/O device access attempt to provide detailed audit logs and incident tracking records.

HIPAA Requirement - 164.308(a)(3)(i) - [Workforce Security](#)

Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to ePHI.

[How Sanctuary Addresses HIPAA Requirements](#)

Sanctuary's flexibility enables policies to be set at a high level or all the way down to device class, specific device or application to users, user groups or a particular computer.

HIPAA Requirement- 164.308(a)(3)(ii)(A) - [Authorization and/or Supervision](#)

Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.

[How Sanctuary Addresses HIPAA Requirements](#)

Sanctuary enforces policies to authorize access to electronic protected health information at the device class, specific device or application to users, user groups or a particular computer.

HIPAA Requirement - **164.308(a)(3)(ii)(B)** - *Workforce Clearance Procedure*

Implement procedures to determine that the access of a workforce member to ePHI.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enables the implementation of procedures to effectively match workforce member to appropriate access rights.

HIPAA Requirement - **164.308(a)(3)(ii)(C)** - *Termination Procedures*

Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enables the termination of workforce member access to applications and devices used on endpoints through simple administration console.

HIPAA Requirement - **164.308(a)(4)(i)** - *Information Access Management*

Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enforces application and device use policies so that only authorized applications or devices can execute or connect to an endpoint.

HIPAA Requirement - **64.308(a)(4)(ii)(A)** - *Isolating Health Care Clearinghouse Function*

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enables the authorization of only appropriate users to access clearinghouse applications and related workstations' devices.

HIPAA Requirement - **164.308(a)(4)(ii)(B)** - *Access Authorization*

Implement policies and procedures for granting access to ePHI, for example, through access to a

workstation, transaction, program, process, or other mechanism.

How Sanctuary Addresses HIPAA Requirements

Sanctuary implements and enforces policies for related data access authorization across programs, workstations and devices.

HIPAA Requirement - 164.308(a)(4)(ii)(C) - *Access Establishment and Modification*

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

How Sanctuary Addresses HIPAA Requirements

Sanctuary implements and enforces policies for related data access authorization across programs, workstations and devices and enables access rights to be immediately changed for any user, user group, machine, program or related I/O device.

HIPAA Requirement - 164.308(a)(5)(ii)(B) - *Protection from Malicious Software*

Implement procedures for guarding against, detecting, and reporting malicious software.

How Sanctuary Addresses HIPAA Requirements

Sanctuary implements and enforces policies to prevent dissemination of malicious code and sets appropriate reporting on any execution attempts per user or per machine.

HIPAA Requirement- 164.308(a)(5)(ii)(C) - *Log-in Monitoring*

Implement procedures for monitoring log-in attempts and reporting discrepancies.

How Sanctuary Addresses HIPAA Requirements

Sanctuary enforces monitoring and reporting procedures with complete log of any attempt to access a program or device.

HIPAA Requirement - 164.308(a)(5)(ii)(D) - *Password Management*

Implement procedures for creating, changing, and safeguarding passwords.

How Sanctuary Addresses HIPAA Requirements

Sanctuary complements password policies with central access management for all users to applications and I/O devices.

HIPAA Requirement - **164.308(a)(6)(ii)** - *Response and Reporting*

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

How Sanctuary Addresses HIPAA Requirements

Sanctuary identifies any attempt to access a program or device and tracks the user responsible for making the attempt.

HIPAA Requirement- **164.308(a)** *Evaluation*

Implement policies and procedures to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

How Sanctuary Addresses HIPAA Requirements

Sanctuary provides the capability to establish periodic reporting that maps users to applications and I/O devices that they have accessed.

HIPAA Physical Safeguards

HIPAA Requirement - **164.310(a)(2)(ii)** - *Facility Security Plan*

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

How Sanctuary Addresses HIPAA Requirements

Sanctuary complements policies safeguarding physical access to machines through I/O device access management per user, user group or machine.

HIPAA Requirement - **164.310(a)(2)(iii)** - *Access Control and Validation Procedures*

Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

How Sanctuary Addresses HIPAA Requirements

Sanctuary implements procedures to control and validate access to programs based on a user's role,

with the ability to enable temporary and/or on-the-fly access to certain programs by specific users.

HIPAA Requirement - 164.310(a)(2)(iv) - *Maintenance Records*

Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).

How Sanctuary Addresses HIPAA Requirements

Sanctuary records all access granted to any I/O device per user, user group and machine.

HIPAA Requirement - 164.310(b) - *Workstation Use*

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

How Sanctuary Addresses HIPAA Requirements

Sanctuary centrally authorizes specific users access to certain removable devices or applications.

HIPAA Requirement - 164.310(d)(2)(ii) - *Media Re-Use*

Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

How Sanctuary Addresses HIPAA Requirements

Sanctuary's patent-pending I/O bi-directional Shadowing tracks information as it is read from or written to floppy, CD/DVD and removable devices.

HIPAA Requirement- 164.310(d)(2)(iii) - *Accountability*

Implement procedures to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

How Sanctuary Addresses HIPAA Requirements

Sanctuary provides comprehensive logging of user access and tracks information as it is read from or written to floppy, CD/DVD and removable devices.

HIPAA Technical Safeguards

HIPAA Requirement - 164.312(a)(2)(i) - *Unique User Identification*

Implement procedures to assign a unique name and/or number for identifying and tracking user identity.

How Sanctuary Addresses HIPAA Requirements

Sanctuary centrally manages all user access to applications and removable devices throughout the entire organization.

HIPAA Requirement - 164.312(b) – *Audit Controls*

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

How Sanctuary Addresses HIPAA Requirements

Sanctuary logs all access attempts to applications or removable devices that contain or use ePHI.

HIPAA Requirement - 164.312(c)(2) – *Integrity*

Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

How Sanctuary Addresses HIPAA Requirements

Sanctuary prevents data alteration by allowing only authorized users to access relevant applications. All access is logged.