adaxes

Softerra Adaxes

Enterprise Directory Solution

HIPAA COMPLIANCE

Achieving HIPAA Compliance with Adaxes

The Health Insurance Portability and Accountability Act (HIPAA) is a set of standards created by Congress designed to safeguard protected health information (PHI) and accelerate the adoption of electronic health record (EHR) systems among providers. The HIPAA has not been rigorously enforced in the past, until new act called HITECH (The Health Information Technology for Economic and Clinical Health Act) was enacted and became effective in February 2010. The HITECH Act widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for noncompliance; and it provides for more enforcement. Furthermore, HIPAA security and privacy standards are now extended to business associates (the organizations contracting with a covered entity that electronically create, store or transmit individually identifiable health care information).

To ensure a successful HIPAA audit, healthcare organizations need to setup the procedures and controls for security and integrity of PHI. One of the key factors to that is the ability to show that PHI is secured through reliable access control and monitoring.

The following table shows how Adaxes helps to sustain HIPAA/HITECH compliance.

HIPAA Section Number	Section Description	Adaxes Assistance
164.308(a)(1)(ii)(A)	**Risk analysis** (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	• Role-based access control • AD reports and report overviews, like risk analysis, inactive accounts, etc.
164.308(a)(1)(ii)(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).	• Role-based access control • Access restrictions in the Web Interface • Notifications on critical events • Approval-based workflow
164.308(a)(1)(ii)(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.	• Notifications on critical events • Approval-based workflow • Extensive logging of AD management history • AD reports and report overviews
164.308(a)(3)(ii)(A)	**Authorization and/or supervision** (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	• Web Interface for AD • Access restrictions in the Web Interface • Approval-based workflow • Extensive logging of AD management history • AD reports
164.308(a)(3)(ii)(B)	**Workforce clearance procedure** (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	• Role-based access control • AD reports

The following table shows how Adaxes helps to sustain HIPAA/HITECH compliance.

HIPAA Section Number	Section Description	Adaxes Assistance
164.308(a)(3)(ii)(C)	**Termination procedures** (Addressable). Implement procedures for terminating access to electronic protected health information 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.	• Automated deprovisioning of terminated employees • AD reports and report overviews like inactive accounts, disabled accounts, etc. • Automated AD cleanup
164.308(a)(4)(ii)(A)	**Isolating health care clearing house functions** (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	• Role-based access control • Web Interface for AD • Access restrictions in the Web Interface • Business Units
164.308(a)(4)(ii)(B)	**Access authorization** (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	• Role-based access control • Access restrictions in the Web Interface • Automated group membership management
164.308(a)(4)(ii)(C)	**Access establishment and modification** (Addressable). 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.	• Role-based access control • Automated delegation of permissions via automated group membership • Automated execution of custom scripts
164.308(a)(5)(ii)(C)	**Log-in monitoring** (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	• Logging of failed log-in attempts • Reporting on failed log-in attempts • Automated account blocking after certain amount of failed log-in attempts
164.308(a)(5)(ii)(D)	**Password management** (Addressable). Procedures for creating, changing, and safeguarding passwords.	• Enhanced management of fine-grained password policies via automated group membership • Auto-generation of random passwords in compliance with password policies • Reporting and notifications on password changes and password resets • Convenient instruments for changing and resetting passwords via Web Interface and Administration Console

The following table shows how Adaxes helps to sustain HIPAA/HITECH compliance.

HIPAA Section Number	Section Description	Adaxes Assistance
164.308(a)(6)(ii)	**Response and Reporting** (Required). 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.	• AD reports and report overviews on critical objects, like inactive accounts, users with never expiring passwords, etc. • Extensive logging of AD management history allowing documenting all securityrelated incidents via Adaxes • Email notifications on critical events for early detection of security incidents • Approval-based workflow

Disclaimer. This document is for information purposes only and should not be treated as an official warranty or certification. The information in this document can be subjected to a change in future with further updates of Softerra Adaxes without prior notice. Therefore, Softerra cannot guarantee the accuracy of any information presented after the publication of the document.