Softerra Adaxes

Enterprise Directory Solution

HIPAA Compliance

make the complex simple

Achieving HIPAA Compliance using 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 non-compliance; 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	Adaxes Assistance
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.	• Email notifications on specific actions in AD • Approval requests for critical actions • Extensive logging of management history and management activity in Active Directory via Adaxes
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.	• Automated delegation of permissions by means of automated group membership • Enhanced distribution of permissions with custom collections of AD objects (Business Units)
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 procedures for terminated • Employees • Reporting on inactive and disabled accounts

HIPAA Section	Adaxes Assistance
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.	• Automated group membership in AD that provides required access rights
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.	• Automated security management 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.	• Reporting on failed logons
164.308(a)(5)(ii)(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	• Enhanced management of fine-grained password policies • Generation of complex random passwords for users • Reporting on password changes and password settings
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.	• Extensive reporting on critical objects that can be the reason of security incidents • Logging of management history and activity in AD that allows documenting all security incidents via Adaxes • Email notifications on critical actions to ensure early detection of security incidents • Requests for approval of the execution of sensitive operations

Disclaimer. The information contained herein is intended solely for the general informational purposes and cannot grant any successful audits. The information is based on sources we believe to be reliable but is not guaranteed by us and does not purport to be a complete or error-free statement or summary of the available data. As such, we do not guarantee the completeness or accuracy of the information. You must evaluate, and bear all risks associated with, the use of any information provided hereunder, including any reliance on the accuracy, completeness, safety or usefulness of such information. Any information contained herein is subject to change without prior notice.