SOLUTION GUIDE

How strongDM Helps with HIPAA Compliance

The **Health Insurance Portability and Accountability Act (HIPAA)** is a federal law that outlines required national standards essential for protecting patient privacy and securing protected health information.

Below are the specific requirements where strongDM helps your organization achieve HIPAA compliance.

Subpart C-Security Standard for the Protection of Electronic Protected Health Information

	Requirement	Detail	StrongDM Feature
§ 164.312	**Technical Safeguards**		
a.1	Access Control	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	strongDM supports Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) policies that can be mapped to administrative safeguards implemented with the Information Access Management Standard. Additionally, strongDM also enables you to grant temporary or just-in-time access with least-privilege by default.
a.2	**Implementation Specifications**		
a.2.i	Unique user identification	Assign a unique name and/or number for identifying and tracking user identity	With strongDM all users must have a unique email address. strongDM allows enables you to authenticate and/or provision users & groups through your identity provider.
a.2.ii	Emergency access procedure	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	With strongDM access is authenticated and authorized through identity. strongDM administrators can set idle timeouts that lock access to the strongDM client and terminate its associated sessions after a desired period of time.
a.2.iii	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	The strongDM Admin UI maintains a list of all users and resources they can access. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes; access can be permanent or temporary. Comprehensive auditing of permissions is available for all access types.

	Requirement	Detail	StrongDM Feature
a.2.iv	Encryption and decryption	Implement a mechanism to encrypt and decrypt electronic protected health information.	strongDM tunnels all connections between local clients and strongDM's proxy server through a single TLS 1.2-secured TCP connection and enhances traditional TLS handshakes with its own secrets between each node, ensuring that Protected Health Information stays encrypted during transit from the storing system to the user. The agent-less architecture of strongDM also means that no electronic health information is ever transmitted outside the customer's network; they fully own and control all gateways and transmission between them.
b	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	strongDM provides session recordings and audit logs for all access to configured data sources. strongDM also records all actions taken within the product itself, providing complete end-to-end auditing of end-user activity with any aspect of information systems, as well as the ability to review and audit these logs. All log storage is encrypted for added security.
c.1	Integrity	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	The strongDM Platform supports the creation and use of Service Accounts to provide the same recorded, auditable access normal users enjoy to automation services and other non-interactive platforms, such as file integrity monitors, and remote configuration management services. Our granluar auditing of queries and sessions also allows for identifying and correcting improper alteration or destruction of information.
a.2.iii	Automatic logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	The strongDM Admin UI maintains a list of all users and resources they can access. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes; access can be permanent or temporary. Comprehensive auditing of permissions is available for all access types.
c.2	**Implementation Specifications**		

	Requirement	Detail	StrongDM Feature
c.2.i	Mechanism to authenticate electronic protected health information.	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	The strongDM Platform supports the creation and use of Service Accounts to provide the same recorded, auditable access normal users enjoy to automation services and other non-interactive platforms, such as file integrity monitors, and remote configuration management services. Our granular auditing of queries and sessions also allows for identifying and correcting improper alteration or destruction of information.
d	Person or entity authentication	Implement procedures to verify that a person or entity seeking access.	strongDM allows you to authenticate and/or provision users & groups through your identity provider, tying our RBAC system to a single source of truth on identity. We also support the use of multi-factor authentication (MFA) as an additional layer of identity-based security in the authentication process.
e.1	Transmission Security	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	strongDM tunnels all connections between local clients and strongDM's proxy server through a single TLS 1.2-secured TCP connection and enhances traditional TLS handshakes with its own secrets between each node, ensuring that Protected Health Information stays encrypted during transit from the storing system to the user. The agent-less architecture of strongDM also means that no electronic health information is ever transmitted outside the customer's network; they fully own and control all gateways and transmission between them.
e.2	**Implementation Specifications**		
e.2.i	Integrity Controls	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	All electronically submitted data is encrypted from end to end to ensure integrity of the data between two points.
e.2.ii	Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	All connectivity between strongDM components (Client, Gateway, API) are encrypted in transit. Additionally, all logging of user activity, queries, and session recordings are fully encrypted.