GOVERLAN | REACH

Extend the reach of your IT services with the industry's
most preferred . powerful . secure solution

HIPAA REGULATORY COMPLIANCE

GOVERLAN.COM

Goverlan Reach & HIPAA Compliance

Goverlan Reach is an on-premises software appliance that allows the management and support of users and computers within your IT infrastructure. Goverlan Reach does not directly handle or process e-PHI data.

Goverlan Reach complies with HIPAA compliance requirements because it operates within your existing security infrastructure. No information about your network or corporate data is transferred outside of your organization. In addition, Goverlan Reach can help in achieving HIPAA regulatory compliance by providing many tools and features to assess and enforce security compliance within an IT infrastructure.

This document both validates the HIPAA compliance of the Goverlan Reach product as well as describes how it can be used to assess and meet compliance requirements.

Meeting and Assessing HIPAA Compliance with Goverlan Reach

■■ How we comply / ■■ How we can help

ADMINISTRATIVE SAFEGUARDS

§164.308 (a)(1) Standard: Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	All actions performed through Goverlan Reach are authenticated and approved based on native Windows security mechanism as configured in Microsoft Active Directory or via local Windows privileges. The application consumes the Windows user account used to spawn the application to authenticate against Windows and gain access to protected resources. Additionally, all actions performed by the Goverlan Reach operator are logged locally or centrally. Audit logs include the full operator identity, time stamps and actions performed. Centralized audit logs can be searched and exported to a report.
§164.308 (a)(3) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, 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 electronic protected health information.	An operator cannot use Goverlan Reach to elevate their own privileges and gain access to protected resources such as e-PHI data. The Windows security layer is used to define the privileges and access level of the solution. By default, the installation of the Goverlan Reach client agent on a remote computer, or the remote desktop access of a remote computer, or the execution of any management tasks on a remote computer, requires local administrative privileges on the remote computer. The reporting of information on the remote computer is only granted based on the configured Windows security access of that resource. **(C) Termination procedures (Addressable)** Goverlan access termination procedures is processed by disabling the user's account in Active Directory. Goverlan Reach can be used to create user termination procedures including disabling accounts and accesses, removing privileges, securing user data and other off-boarding automations.
§164.308 (a)(4) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	**(B) Access authorization (Addressable)** Goverlan Reach is a desktop application that is consumed post login to a workstation. Consequently, only authorized and legitimate users can consume the Goverlan Reach services.
§164.308 (a)(5) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).	**(B) Protection from malicious software (Addressable).** Goverlan Reach can be used to scan remote computers for malicious or prohibited software and uninstall them. **(C) Log-in monitoring (Addressable).** Goverlan Reach can report user login/logout events. **(D) Password management (Addressable).** Goverlan Reach can change user account's passwords on individual accounts or globally.
§164.308 (a)(6)(ii) Implementation specification: 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 or business associate; and document security incidents and their outcomes.	Goverlan Reach provides comprehensive audit logs of users and operators activities that can be used to detect security breaches.

PHYSICAL SAFEGUARDS

§164.310 (a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Goverlan Reach is an on-premises application that can only be consumed by an authenticated and authorized user using the local security configuration. Since Goverlan Reach cannot be accessed without a prior login to a workstation, it complies with these requirements. Goverlan Reach supports SmartCard authentication and redirection in PKI infrastructures.
§164.310 (b) Standard: 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 electronic protected health information.	
§164.310 (c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	

TECHNICAL SAFEGUARDS

§164.312 (a) (1) Standard: 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). **§164.312 (d) Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Goverlan Reach services are consumed through the Goverlan Reach operator console, a desktop application installed on the administrator's machines. This guarantees that Goverlan Reach services cannot be consumed by an un-authenticated / un-authorized user. All actions performed on a remote system are authenticated and approved using the credentials of the Goverlan Reach operators. User access privileges are transferred over to the remote system using the Microsoft SSPI technology (which guarantees the identity of the operator). The features exposed by the Goverlan Reach operator console as well as the behavior of the solution on the client side (such as access approval process and event notifications) are defined and enforced via centrally configured policies through the Goverlan Reach Server.
§164.312 (b) Standard: 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.	Goverlan Reach can centrally log all administrator activity on remote systems including remote desktop access as well as system queries or management tasks. All audits are centrally registered to the Goverlan Reach server and include full operator identity, time stamps and actions performed. Centralized audit logs can be searched and exported to a report.
§164.312 (e) Standard: 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.	All communications between Goverlan Reach Console and Goverlan Reach Client inside the local area network (LAN) are encrypted using AES 256 with symmetric keys which are received using the Ephemeral Diffie-Hellman (DHE) key exchange algorithm. All communication between a Goverlan operator and the managed endpoints go through an SSPI authentication handshake to guarantee the identity of the operator, and provide the ability to impersonate the operator's access privileges to perform local actions. All Internet communications between any parts of the Goverlan system are encrypted using TLS 1.2 originated with an x.509 certificate supplied by the enterprise and signed by an appropriate Certification Authority (CA). In most cases a public trusted CA is recommended.