Soliton®

G/On

HIPAA Compliance Information

Technical Safeguards

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How MailZen Helps
§164.312(a) Access Control	Required	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.	▪ User access to company resources is protected using server-side user directory username/passwords and a physical token for two-factor authentication. ▪ Access from a device or account can be stopped easily by an administrator.
	Required	Unique User Identification Assign a unique name and/or number for identifying and tracking user identity.	▪ G/On uses an existing server-side user directory to identify users and administrators.
	Required	Emergency Access Procedure Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	▪ G/On enables access to company resources from anywhere with internet connectivity. It can be used to provide emergency access to health information.
	Addressable	Automatic Logoff Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	▪ Users are automatically logged out for inactivity after a preset time.
	Addressable	Encryption and Decryption Implement a mechanism to encrypt and decrypt electronic protected health information.	▪ G/On uses 233-bit Elliptic Curve Cryptography (ECC) for authenticating the server, 2048-bit RSA keys for protecting information during the setup of the encryption (key exchange), and 256-bit AES for encrypting the traffic.

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How MailZen Helps
§164.312(b) Audit Controls	Required	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	▪ All remote sessions are logged and easily accessible by administrators.
§164.312(c) Integrity	Required	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	▪ G/On enforces that no user will have access to a given service unless an access policy has been defined to allow the user to access the resource. The access policies can be based on user groups in a user directory, such as AD.
	Addressable	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.	▪ Decrypted data during a remote session is checked for network transmission integrity.
§164.312(d) Person or Entity Authentication	Required	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	▪ User access to company resources is protected using server-side user directory username/passwords and a physical token for two-factor authentication. ▪ G/On enforces that no user will have access to a given service unless an access policy has been defined to allow the user to access the resource. The access policies can be based on user groups in a user directory, such as AD.

Compliance with HIPAA Technical Safeguards

Category	Required/ Addressable	Standards	How MailZen Helps
§164.312(e) Transmission Security	Required	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	▪ G/On uses 233-bit Elliptic Curve Cryptography (ECC) for authenticating the server, 2048-bit RSA keys for protecting information during the setup of the encryption (key exchange), and 256-bit AES for encrypting the traffic. ▪ No data is left on the client device after a remote session ends.
	Addressable	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	▪ Decrypted data during a remote session is checked for network transmission integrity.
	Addressable	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	▪ G/On uses 233-bit Elliptic Curve Cryptography (ECC) for authenticating the server, 2048-bit RSA keys for protecting information during the setup of the encryption (key exchange), and 256-bit AES for encrypting the traffic.