How the Sevan WSA Addresses HIPAA Requirements

A Sevan White Paper

sevan networks

The Health Insurance Portability and Accountability Act (HIPAA) requires that measures to be taken to secure health information that is collected, maintained, used, or transmitted electronically. HIPAA requires that healthcare organizations implement administrative, physical, and technical safeguards that protect the confidentiality and integrity of personally identifiable healthcare information.

The Sevan WSA can provide many of the technical safeguards and security measures required by HIPAA. By protecting the web servers that host the health information, the WSA provides access control, audit, integrity, authentication, and transmission security – the foundation for HIPAA compliance. The WSA safeguards the health information without requiring changes to your applications or the user experience. The WSA can be installed and configured in a few hours.

The Sevan WSA is a hardened security appliance, designed to meet FIPS 140-2 requirements. The Sevan WSA provides: certificate-based user authentication (widely considered the strongest form of authentication), strong encryption, role-based access control, delegated administration, and audit.

The WSA can be operated as a stand-alone device or integrated with your Lightweight Directory Access Protocol (LDAP) directories and Microsoft Active Directory. If you already have an established PKI, the WSA can be quickly and simply integrated into your certificate infrastructure.

The table below summarizes HIPAA technical safeguards and security measures met by the Sevan WSA.

HIPAA Technical Safeguard Standards	**Implementation Specifications** (R) = Required (A) = Addressable	**Sevan WSA features**
§164.312(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).	**(R) – Unique User Identifier.** Assign a unique name and/or number for identifying and tracking user identity.	The WSA authenticates each user through his unique SSL certificate. No two users have the same certificate.
	(R) – Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	The WSA features support a wide range of emergency access. For example, multiple certificates per user; multiple users per account; multiple roles; and even emergency password access.
	(A) – Automatic Logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Optional requirement. The electronic session is terminated by the user closes the browser. A future WSA release will include automatic time-outs.
	(A) – Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information.	Optional requirement. The WSA encrypts all health information before leaving the servers.
§164.312(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.	**(R)** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	The WSA maintains secure audit logs for administrative actions, user activity, system and network events

§164.312(c) – Integrity Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	**(A) – 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 WSA creates a security envelope around the health information. Only authorized users can access the information, thus ensuring the information's integrity. Certificate-based authentication and SSL/TLS security maintain integrity while the information is transmitted.
§164.312(d) – Person or Entity Authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	**(R)** - Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	The WSA uses certificate-based authentication for persons or entities, which is the strongest form of authentication. The certificate can be protected by a PIN, It can be stored on a computer, smart card, or token.
§164.312(e) – 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.	**(A) – Integrity Controls.** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	The WSA protects the integrity of the health information by establishing a SSL/TLS security session between the server and the user's computer. The security session detects in-transit modification of the information.
	(A) – Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Strong SSL encryption ensures confidentiality of transmitted data

Conclusion

Installing a Sevan WSA in front of your web servers can quickly and inexpensively achieve many of the HIPAA Technical Safeguards. The WSA ensures that only the right people gain access to the right health information on the web site. The WSA encrypts all information leaving and entering the web site.

sevan
networks

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com