Dataweavers

HIPAA Compliance Checklist for Sitecore Websites

HIPAA compliance with a signed Business Associate Agreement (BAA) is just one step toward effective governance. To uncover your potential risks, use our checklist to dive deeper on encryption, access controls, risk management, auditing & monitoring.

KEY REQUIREMENT	DESCRIPTION	APPROACH (HOW TO)		HAVE YOU IMPLEMENTED?	
				Yes	No
Encryption	Is the data used in the solution specifically ePHI data, encrypted in transit and at rest. Are they keys appropriately controlled.	**Transport Encryption**	In transit – SSL	☐	☐
		Encryption At Rest	At rest – TDE	☐	☐
		Secure key / cert management	Key Vault	☐	☐
Access Controls	Does the solution have suitable access controls in the application where roles and responsibilities are mapped. Does the solution at the infrastructure level have the appropriate access controls. Are enhanced identity solutions used including the use of MFA, to protect user credentials and access.	**Rolebased**	Extensive RBAC	☐	☐
		Isolated ePHI Data	Isolated Customer Data	☐	☐
		Advanced Identity	Azure AAD for CM with 2FA	☐	☐
Risk Management	Appropriately implemented Risk management framework, including assessment, controls, monitoring, improvement, training, and response. Alignment with the High trust CSF and control assessment.	**Multilayer Network**	Defence in Depth	☐	☐
		Ongoing Review	Regular Control Review	☐	☐
		WAF	WAF Policies	☐	☐
		DDOS/BOT	BoT and DDOS Protection	☐	☐

This is a simple check list designed to help identify if you may have areas that need to be addressed in your Sitecore Solution alone. This does not replace a full CSF assessment that you may need to evaluate your organisational position for HITRUST compliance.

KEY REQUIREMENT	DESCRIPTION	APPROACH (HOW TO)		HAVE YOU IMPLEMENTED?	
				Yes	No
Auditing	Application-level auditing / logging to record which users performed which actions. Infrastructure auditing to identify which processes or operational team members access and or modify infrastructure configuration. Data access auditing.	**Infrastructure Auditing** **Solution Auditing**	Azure Auditing SQL Auditing	☐ ☐	☐ ☐
Monitoring	Suitable monitoring platforms and observability platforms that can provide advanced warning of security incidents and alerting, that can be actioned. This should cover the application layer, the underlying infrastructure layer, the network, and the ingress points.	**Application Alerts** **Filtering** **Ongoing Scans** **SIEM**	Application Insights Intelligent Filtering Defender for Cloud Central NOC & Tooling	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐

This is a simple check list designed to help identify if you may have areas that need to be addressed in your Sitecore Solution alone. This does not replace a full CSF assessment that you may need to evaluate your organisational position for HITRUST compliance.

Did you answer “No” or you’re Not Sure?

If you answered “No” or you’re not sure about 5 or more questions in our checklist, it’s time to better understand your platform and its compliance requirements.

Get started

Discover how Dataweavers can help.

www.dataweavers.com

Dataweavers