SITECORE

WHITEPAPER

Sitecore SaaS DXP and HIPAA

Shared Responsibility Whitepaper

Introduction

At Sitecore, we understand the value of data and the importance of protecting it. We know our customers and the diversity of digital properties you manage across all verticals, as well as the first-party data you collect to best understand and reach your audiences. We know you are facing rapidly evolving privacy regulations and serious consequences for violations. We understand the competitive premium now placed on management of customer data and trust-based relationships between organizations and their customers.

Sitecore is committed to a security and privacy-first philosophy, following ethical data practices and emulating that in our own internal compliance framework, as well as implementing privacy-by-design features and security-as-default in our products and services. Having effective data governance, with privacy and security controls that our customers trust, is not a one-time effort; it requires ongoing monitoring of all Sitecore data flows, continuously improving our processes, and optimizing data integrity.

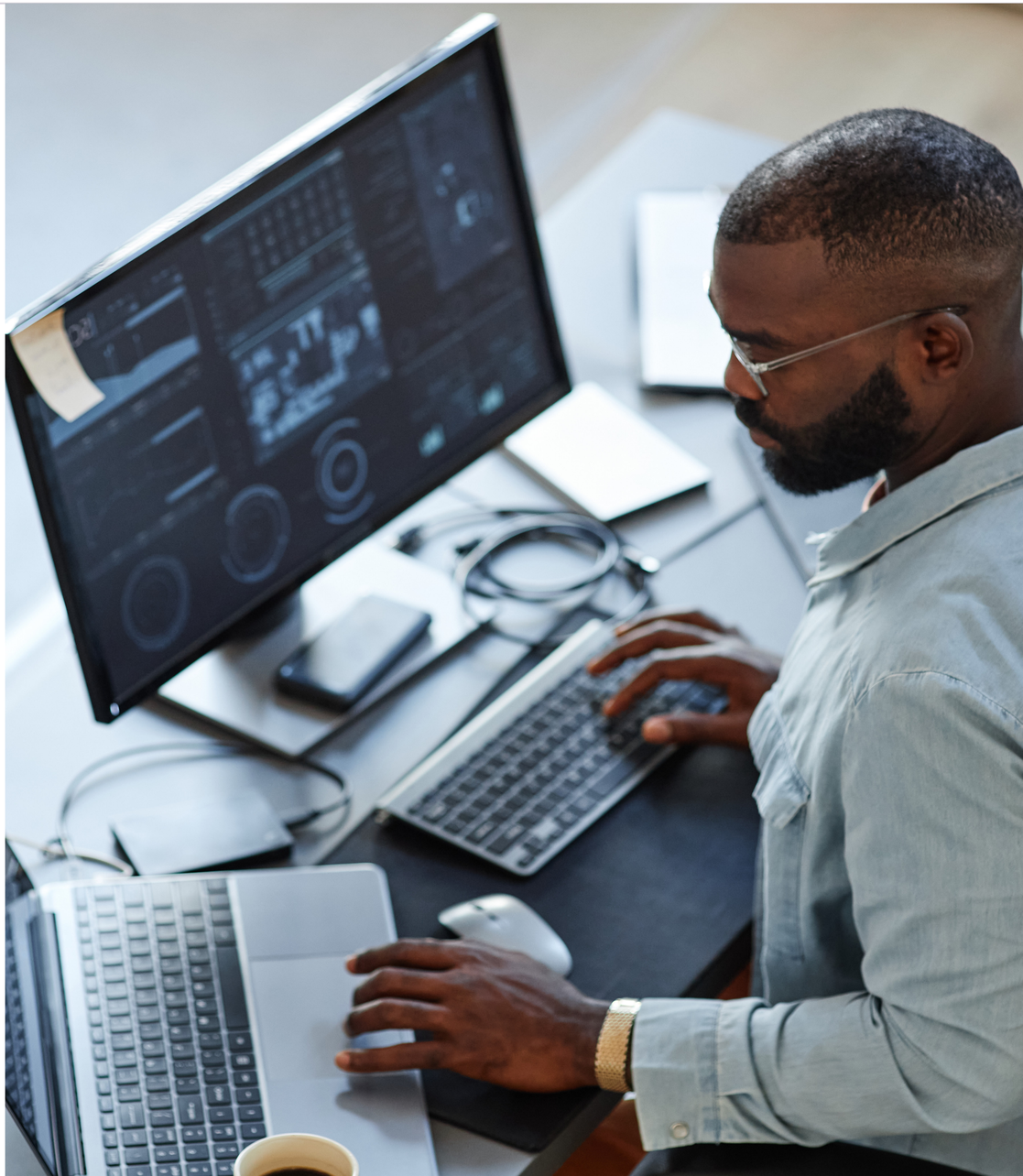
Privacy is built into services as part of our Secure Software Development Lifecycle, a process designed to help assess risk and design product functionality and configurability that addresses privacy and security compliance needs. Implementing strong security protocols, conforming to international security standards, with policies and operational processes overseeing all aspects of our business practices, allowing us to ensure data protection throughout the data lifecycle.

Helping you ensure data security

Keeping your data secure is a fundamental part of Sitecore compliance – we must take care of data and maintain trustworthy operations. At Sitecore, we incorporate security into our products and best practices into everything we do, including robust information security practices and secure development practices.

As your partner in compliance, we want to continually support your efforts towards secure data operations and adopting practices in line with Security by Design principles – prioritizing confidentiality, integrity, availability, and resilience as the core pillars of information security. We support the use of strong security measures to protect personal data throughout the product lifecycle, including encryption of data at rest and in motion.

Fundamentally, your customers want to know, “If I share my personal data with you, will you keep it safe and secure?”



The protection of personal data including PHI is a shared responsibility between Sitecore and our customers. In line with these efforts, we have created this whitepaper to describe the shared responsibilities between Sitecore and our customers under the HIPAA Security Rule.

HIPAA Shared Responsibility Matrix

Sitecore's **HIPAA Shared Responsibility Matrix** and has been designed for use with all our HIPAA Ready SaaS products*.

*HIPAA Ready Products include

- Sitecore CDP
- Sitecore Personalize
- Sitecore XM Cloud
- Sitecore Content Hub

General Rules	Sitecore Responsibilities	Customer Responsibilities
Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; Identify and protect against reasonably anticipated threats to the security or integrity of the information; Protect against reasonably anticipated, impermissible uses or disclosures; Ensure compliance by their workforce.	All privacy, data protection, cyber compliance, and data governance activities are led by Sitecore's Chief Digital and Information Officer and supported by subject-matter experts. This includes product security, privacy and data protection counsel, IT security, security engineering, and security operations.	Sitecore recommends that its customers follow industry best practices in their policies and procedures to ensure the confidentiality, availability and integrity of PHI in their licensed Sitecore products.

Administrative Safeguards	Sitecore Responsibilities	Customer Responsibilities
Security Management Process	Sitecore has dedicated security and data protection teams and is compliant with multiple security frameworks including ISO 27001, ISO 27017, ISO 27018, CSA STAR, HIPAA, SOC 1 & 2 and retains a third-party vendor for independent internal audits as required for ISO 27001 certification. Sitecore is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and Sitecore's internal risk and compliance team.	Sitecore recommends that its customers make independent security determinations that incorporate use of the Sitecore platform and utilize the security measures available on the Sitecore platform to reduce the risks to customer data including PHI.
Security Personnel	Sitecore has an appointed Chief Cyber Security Office who performs the duties of a HIPAA Security Officer.	–
Information Access Management	Sitecore products allow customers to monitor system activities, providing organizations with full visibility into user interactions within the Sitecore platform.	Sitecore recommends that its customers regularly use the features available on the Sitecore platform to monitor user activity with customer data.
Workforce Training and Management	All Sitecore personnel must complete security awareness training, including HIPAA specific training as part of onboarding and as part of Sitecore's recurring annual training curriculum.	Sitecore recommends that its customers train their workforce on the appropriate handling of PHI data, in Sitecore's products.

Physical Safeguards	Sitecore Responsibilities	Customer Responsibilities
Facility Access Control	Sitecore has partnered with leading cloud providers such as Microsoft Azure and Amazon Web Services to provide hosting services for our SaaS and PaaS product offerings. These cloud providers are compliant with many security frameworks.	Sitecore recommends that its customers deploy consistent practices for physical control security at each workplace from which Sitecore products are accessible.
Workstation and Device Security	Sitecore personnel may only access Sitecore's network using Sitecore-issued devices or end-user devices that support Sitecore's current security requirements. Standards for end-user devices include protective controls and specific configurations, such as anti-virus software, patching, and required operating system or other software versions. Sitecore-issued machines are configured to automatically receive upgrades.	Sitecore recommends that its customers ensure devices which access Sitecore products have appropriate antivirus and security controls installed in line with industry best practice.

Technical Safeguards	Sitecore Responsibilities	Customer Responsibilities
Access Control	Sitecore has implemented organizational and technical controls to secure authentication and authorize permission for access to processing environments, including using centralized directory services and role-based access controls. Sitecore provides customers with a variety of features for configuring access controls to preserve platform integrity and safeguard customer data. Together with internal policies and procedures, Sitecore ensures the secure handling of data.	Sitecore customers are advised to configure access management from the Sitecore Cloud Portal. Learn more at: https://doc.sitecore.com/portal/en/developers/sitecore-cloud-portal/introduction-to-the-sitecore-cloud-portal.html
Audit Controls	Sitecore maintains detailed audit logs of user activity, providing organizations with a systematic means to monitor and review user interactions within the Sitecore platform. By prioritizing the security, integrity, and reliability of these logs, Sitecore supports customer investigations into and resolution of customer inquiries.	Sitecore recommends customers regularly use the features available on the Sitecore platform to monitor user activity with customer data. Sitecore offers a method to review events and activity via Sitecore's Common Audit Log. Learn more at: https://doc.sitecore.com/portal/en/developers/sitecore-cloud-portal/sitecore-common-audit-log.html
Integrity Controls	Sitecore has implemented thorough data backup and recovery systems to protect against data loss as well as security measures to ensure the confidentiality and security of data within its platforms.	Sitecore recommends that customers implement appropriate policies and procedures to protect electronic protected health information.
Transmission Security	Sitecore has implemented encryption measures for customer data both in transit and at rest in alignment with industry standards for safeguarding data. Sitecore employs Transport Layer Security (TLS), ensuring that PHI is securely transmitted over public networks. TLS encryption provides a robust shield against unauthorized access during data transmission, aligning with industry best practices for safeguarding sensitive healthcare information. Regarding data at rest, Sitecore leverages the advanced encryption capabilities of cloud native tools, implementing AES-256 encryption.	Sitecore recommends customers review and familiarize themselves with Sitecore's data privacy and data encryption practices which can be found in our documentation site: https://doc.sitecore.com/

About Sitecore

Sitecore is a global leader of end-to-end digital experience software. Unifying data, content, commerce, and experiences, our SaaS-enabled, composable platform empowers brands like L'Oréal, Microsoft, and United Airlines to deliver unforgettable interactions across every touchpoint. Our solution provides the cutting-edge tools brands need to build stronger connections with customers, while creating content efficiencies to stand out as transformation and innovation leaders.

Experience more at sitecore.com.

Legal Disclaimer

While every effort has been made to ensure the accuracy and completeness of the information contained herein, Sitecore makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the content. Any reliance you place on such information is therefore strictly at your own risk. We recommend consulting with a qualified legal professional for advice specific to your circumstances.

SC-005-SitecoreSaaSDXPandHIPAA-WP-EN-1024-SC