Kontent.ai

Kontent.ai provides HIPAA compliance for customers.

Kontent.ai is committed to maintaining confidentiality, integrity, and availability of data that customers entrust into our product. To help assure our healthcare customers of the high standards we put into the protection of protected health information (PHI), we have prepared this whitepaper that explains how Kontent.ai addresses the requirements of the HIPAA Security Rule.

Executive summary.

Kontent.ai application has been developed with security and privacy in mind. It contains security features that help customers protect their data. In addition, the internal operation of Kontent.ai as an organization follows industry standards and best practices to ensure that customer data, including PHI, remains secure.

- Kontent.ai has a strong emphasis on security, coordinated by the internal security team led by CISO
- The security program of Kontent.ai is focused on protecting customer data and covers all areas of application, infrastructure, information, physical, and supply chain security
- As an assurance, ISO/IEC 27001, 27017, and SOC 2 Type 2 certifications/audit reports are provided to customers upon a request

How to work with this material.

Kontent.ai has prepared this whitepaper to inform customers about:

- How Kontent.ai addresses the specific requirements internally
- What further steps can customers take to secure PHI when using Kontent.ai application

These elements comprise a shared responsibility model over PHI in Kontent.ai cloud offering. The table below can be read by rows, where every row covers a specific requirement, Kontent.ai internal operation and further recommendations. It is essential to review those recommendations and utilize all security features and functions of Kontent.ai application in order to protect PHI.

The table covers merely relevant requirements we have chosen to demonstrate compliance and is not an exhaustive list. Customers are encouraged to contact Kontent.ai through their customer representative or security@kontent.ai should they seek further answers.

Overview of the shared responsibilities.

General rules	Kontent.ai Controls and comments	Kontent.ai Recommendations
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.	Kontent.ai has implemented organizational, physical, technical, and administrative controls and safeguards to ensure ongoing confidentiality, integrity, and availability of any customer data, including PHI.	Ensure that Kontent.ai application is embedded into a secure architecture of the customer environment. All data entry and output areas should be properly secured. Customers are recommended to develop and keep adequate documentation regarding such data flows and their usage of Kontent.ai application.

Ensure compliance by their workforce.	There is a policy framework and security and privacy awareness program in place. These ensure that the workforce is informed and required to be compliant with protecting customer data, including PHI.	The customer workforce that has access to Kontent.ai application should be well-educated, informed, and trained on handling PHI and specific Kontent.ai controls and features. Kontent.ai Learn https://kontent.ai/learn/ provides e-learning, training, certifications, and tutorials explaining all relevant areas.
Maintenance	There is a regular review of controls in place and an ongoing security program that continuously works towards improving the control health and security awareness and reacts to business changes that could affect internal security in Kontent.ai.	Customers should review their controls on a regular basis, including those used in combination with Kontent.ai application.
Administrative safeguards		
Security Management Process	Kontent.ai maintains a certified Information Security Management System that is aligned with international standards such as ISO/IEC 27001, 27017, and Trusted Services Criteria. An integral part of the System is a risk analysis that is performed on a continuous basis, with a major review done at least annually or when an important business change occurs. Kontent.ai has defined and approved Risk Appetite Statement and works with quantifiable methods to calculate the potential loss.	Kontent.ai recommends customers perform their own risk analysis with respect to any PHI they seek to process in Kontent.ai application and in the spirit of other items in this whitepaper.

Assigned security responsibility	Kontent.ai designated a role of CISO and Security Team to oversee the security of information assets, infrastructure, product, suppliers, and physical locations.	—
Workforce security	Kontent.ai has implemented processes to ensure that only authorized individuals gain access to important assets. These include background checks, onboarding, training, access reviews, and management on a regular basis or during a change of assignment or termination.	Kontent.ai recommends only granting access to the application to authorized individuals and regularly checking if they are still necessary.
Information Access Management	There are strict rules governing the access to any customer data, including potentially PHI. The access is utilized only in disaster and in support cases based on customer's designation and approval.	The roles and permissions in Kontent.ai can be set up in a granularity that reflects the customer's needs. Kontent.ai recommends following the least privilege principle when designing the permission model in Kontent.ai application. For more information, see kontent.ai/learn/tutorials/set-up-kontent-ai/set-up-team-and-collaborate/roles/. Furthermore, taxonomies (kontent.ai/learn/tutorials/manage-kontent-ai/taxonomies/model-taxonomies-right/) and/or content groups (kontent.ai/learn/tutorials/manage-kontent-ai/content-modeling/organize-elements-with-content-groups/) can be used for organizing content so that PHI is clearly distinguished in the system.

Security awareness and training	There is a comprehensive security culture program that comprises security awareness training, tests, gamification, recognitions, and more.	It is recommended to provide additional training for relevant roles responsible for securing and working with the PHI within Kontent.ai application. Refer to Kontent.ai Learn for relevant training and documentation on security features: kontent.ai/learn/
Security incident procedures	Kontent.ai utilizes complex processes for security incident management. Incidents are managed by their severity, triaged, documented, and communicated. The process follows NIST recommendations and ISO 27001 framework.	In case of a security incident concerning Kontent.ai application or customer data there, customers are advised to contact the support without undue delay.
Contingency plan	Contingency plans have been established and are tested on a regular basis during disaster recovery drills.	Kontent.ai recommends customers to maintain their own contingency plans concerning Kontent.ai application and the data stored in it. Customers can also create their own backups to speed up the recovery phase in some scenarios and also have better control over recovery (e.g., in case of corruption by their own script): kontent.ai/learn/tutorials/references/backup-and-restore/#a-options-to-manage-backups-on-your-end
Evaluation	Kontent.ai performs both internal and external evaluations of security, including audits, reviews, vulnerability assessments, and penetration tests.	For their own audit needs, customers may request the latest copies of penetration testing done on Kontent.ai application, as well as SOC 2 Type 2 report or security certificates. These are shared under an NDA.

Physical safeguards		
Facility access controls	Customer data are not stored in Kontent.ai facilities but in MS Azure data centers. More information about facility access controls can be found at: learn.microsoft.com/en-us/azure/security/fundamentals/physical-security	Access controls to facilities from which customer personnel can access Kontent.ai application and PHI stored there should also be addressed by customer security policies and controls.
Workstation use	Kontent.ai has established a policy framework that governs the acceptable use of assets as well as security controls that must be in place to secure customer data, including PHI.	Similar to Kontent.ai internal rules, customers are advised to develop their own policies and procedures in compliance with § 164.310 b)
Workstation security	There is a strict limitation on which workstations may be used to access customer data. These employ security controls to prevent unauthorized users from accessing them.	The workstations from which customers will access PHI in Kontent.ai application should be adequately protected.
Device and media controls	Customer data are never stored on removable or mobile media, and storage is protected by multiple sets of controls in MS Azure Data Centers. For reference, more information can be found at: learn.microsoft.com/en-us/azure/security/fundamentals/physical-security	Customers are recommended to adequately protect all device and media which stores PHI. There should be a focus on devices and media that process data which are ultimately stored in Kontent.ai application.

Technical safeguards		
Access control	Kontent.ai employs access controls to govern access to customer data, including PHI. Users are uniquely identified and authenticated using multifactor authentication, and their authorization rights are checked. There are procedures in place for retrieving data in emergencies and disasters.	Kontent.ai provides Single Sign On (SSO) integration or utilizes unique user names. Furthermore, it is possible to set up roles and assign them permissions in Kontent.ai application. This way, access to the PHI can be managed. More information on setting up roles and permissions can be found in Kontent.ai Learn: kontent.ai/learn/tutorials/set-up-kontent-ai/set-up-team-and-collaborate/roles/ There is a session expiration in place, and all data is encrypted by default. To ensure the confidentiality of data during the whole content lifecycle, it is possible to restrict access to the published content. kontent.ai/learn/tutorials/develop-apps/build-strong-foundation/restrict-public-access/ Customers should consider using customizable expiration time for API keys to manage the security of their integrations.
Person or entity authentication	All-access requests to PHI are subject to verification. Internally in Kontent.ai, access is limited to the cases of disaster recovery and only for designated personnel dealing with the issue.	Kontent.ai provides Single Sign On (SSO) integration, enforces a strong password policy if SSO is not utilized, and supports multifactor authentication.
Transmission security	Access to Kontent.ai resources by end users is encrypted. More information can be found in Kontent.ai Learn: kontent.ai/learn/tutorials/references/data-encryption/#a-encryption-in-transit.	Customers are required to use browsers and workstations in versions that support the used cryptographic protocols.

Information in this whitepaper is for informational purposes only and does not constitute legal advice. It discusses how Kontent.ai helps with compliance of key requirements from the HIPAA Security Rule. The information provided is based on general principles of United States law and regulations as of the publication date. The information provided in this Whitepaper may not reflect recent changes in HIPAA regulations or legal interpretations. Readers are advised to consult legal professionals for tailored advice and guidance. **While efforts have been made to ensure accuracy, no representation or warranty, express or implied, is made regarding completeness, accuracy, reliability, or suitability. Kontent.ai is not liable for any direct, indirect, incidental, consequential, punitive, or special damages arising out of or in connection with the use of this Whitepaper or reliance on the information contained herein.** Customers are responsible for their own compliance with HIPAA and any other regulations and for ensuring that Kontent.ai application is used in compliance with applicable laws.

Kontent.ai

About Kontent.ai.

Kontent.ai is the headless CMS that enables organizations to have complete control over content to speed up time to market and engage meaningfully with audiences across channels.

With offices in New York, London, Amsterdam, Brno, and Sydney, Kontent.ai supports global customers including Zurich Insurance, Algolia, and Oxford University. Kontent.ai is a Microsoft partner and MACH Alliance member, recognized by both Gartner and Forrester. Visit kontent.ai to learn more about how we empower leading organizations.

SCHEDULE YOUR DEMO →