We are on the same team!

We understandably receive a lot of questions from our customers as to how Preservica, as a cloud service provider, is taking appropriate action for the protection and confidentiality of our client data.

The responsibilities detailed in this paper are applicable across our entire service offering but are specifically written in the context of Preservica Cloud.

At a high level, Preservica handles security of the applications themselves, the systems they run on, and the environments those systems are hosted within. We ensure your systems and environments are compliant with relevant standards, including ISO 27001:2022, Cyber Essentials Plus and SOC2, as required.

You, our clients, manage the information within your accounts, the users and user accounts accessing your data, and the management of records within the application. When using our services, you are responsible for ensuring your business is meeting your own compliance obligations.

In the cloud, the security of your data on our services is a joint responsibility. We developed these shared responsibilities to outline what actions we take to protect your data, and what you need to do.

	What we do	What you need to do
Governance, Risk and Compliance	Ensure Preservica has established and tested business continuity and incident response plans. Ensure our data centre partners meet or exceed Preservica's compliance requirements. Provide information about our compliance through our Trust Centre. Ensure our offerings meet or exceed the certifications and accreditations that we claim. This includes ISO 27001:2022, SOC 2 Type II and more. See our Trust Centre. Adhere to our Sustainability Charter to ensure our continued success as a business.	Operate within the law of the jurisdiction in which you operate. Assess the suitability of our services based on the information we provide. Understand the risks associated with using a SaaS service as well as the benefits.
Infrastructure	Provide you with access to our services according to our SLA. Ensure that our infrastructure is configured with appropriate network security technologies.	Understand that Preservica operates on cloud infrastructure provided by a 3rd party (AWS or Azure). Ensure suitable endpoint protection is in place on the devices you use to access Preservica.
Data	Access your data only if there is a specific need to do so. Notify you of any breach we become aware of that affects your data. Maintain backups and recovery plans to meet our RPO and RTO objectives. Ensure your data is encrypted at-rest and in-flight.	Understand the regulatory and compliance needs of the data you wish to ingest. Only ingest data that is permitted given the compliance of the Preservica service. Ensure your staff are aware of their obligations under the Acceptable Use Policy.

Commercial in Confidence | Copyright © Preservica 2024, all Trademarks acknowledged.

	What we do	What you need to do
	Ensure the integrity of data that you ingest through checksums and other cryptographical techniques.	If you choose to use a custom domain to access the service, you may need to collaborate with our Operations team for SSL certificate renewals. Manage the data and metadata that you ingest into the service according to your organization's data and records management policies.
Security Operations	Manage security incidents and notify you of any incidents that affect your environment. Receive and manage vulnerability reports related to our service. Monitor our platform for bad or malicious actors, including insider threats.	Monitor your user accounts and activity logs for malicious activity. Be aware of the risks of social engineering, phishing and other attack vectors that could result in your users inadvertently revealing their log in credentials.
Application Security	Develop and deploy security tools and functionality that empower you to manage users, roles and permissions effectively. Remediate any vulnerabilities in the service in a timely manner using a risk-based approach.	Configure and manage roles according to your business needs. Configure access control and other security controls according to your own security policies. Add, delete, modify, and periodically review users of the service according to your security policies. Notify Preservica of any unauthorized use of your organization accounts.

Commercial in Confidence | Copyright © Preservica 2024, all Trademarks acknowledged.

HIPAA Responsibilities

Where you store protected health information (PHI), as defined under the Health Insurance Portability and Accountability Act (HIPAA), in Preservica Cloud, the responsibilities below apply in addition to those above.

Preservica acts as your business associate under HIPAA and signs a Business Associate Agreement (BAA) with you. If the BAA differs from this model, the BAA takes precedence.

	What we do	What you need to do
Governance, Risk and Compliance	Sign a BAA with you before you store PHI. Maintain a HIPAA security program, including risk analysis, workforce training and a designated Security Official. Ensure data centre partners that handle PHI have BAAs in place with Preservica.	Include Preservica in your HIPAA risk analysis.
Infrastructure	Ensure our hosting providers maintain physical safeguards for the facilities that house your PHI.	*No additional responsibilities.*
Data	Use and disclose PHI only as permitted by our BAA. Notify you of any breach of PHI within the timeframe set in our BAA. Return or destroy your PHI at the end of our agreement.	Do not ingest PHI until a BAA is in place. Handle individuals' requests to access or amend their PHI, if it is part of a Designated Record Set (DRS), and make any breach notifications HIPAA requires of you. Identify and tag records containing PHI, when you ingest them, and keep those tags accurate.
Security Operations	Log and review access to systems that contain PHI. Ensure Workforce monitoring is performed. Train our personnel on HIPAA security awareness.	Train your users on HIPAA security awareness. Monitor your Workforce in accordance with local policies.
Application Security	Support multi-factor authentication (MFA), single sign-on and session timeouts.	Grant users only the minimum necessary access to PHI according to their role. Enable MFA and session timeouts for all users who can access PHI.

Commercial in Confidence | Copyright © Preservica 2024, all Trademarks acknowledged.