HIPAA Compliance

HIPAA and the later adoption of the HITECH Act established through the Department of Health and Human Services is a set of Privacy and Security Rules governing the handling of Protected Health Information (PHI). Under these rules, "Covered Entities"[^1] are required to meet certain security and data requirements in order to keep PHI safe.[^2] Covered Entities who utilize third-party entities (such as a Service Provider) who will "create, receive, maintain or transmit" PHI in providing a function, activity, or service on behalf of that Covered Entity are defined as a "Business Associate." In most cases, any Business Associate must enter into a Business Associate Agreement (BAA) with the Covered Entity.

Security and privacy for our customers is one of the key tenants of our Frame Desktop as a Service (DaaS) platform. Our security and compliance team, in coordination with Frame Legal, has determined the necessary deployment models, responsibilities, and actions a Covered Entity or Business Associate of Frame must follow in order for Frame to execute BAAs.

The architectural design requirements for Frame described below are required for Frame to enter into a BAA.

Deployment Requirements

- Covered Entities may use Frame-supported public cloud platforms or on-premises Nutanix infrastructure. Public cloud Frame deployments must utilize the Bring Your Own (BYO) infrastructure capability.
- Covered Entities must leverage the full Private Networking configuration option when deploying Frame. Any ingress into the Frame-managed workload VMs and egress from the workload VMs must be controlled through the customers' security appliances.
- If applicable, Frame deployments may use Enterprise Profiles.
- Covered Entities must bring their own SAML2-based identity provider (IdP). These entities may not use my.nutanix.com or the Frame IdP as identity providers.
- User authorization to PHI must be enforced by the Covered Entity's applications. These entities may not rely solely on Frame's Role-based Access Control (RBAC) to determine which users have access to PHI.
- Frame Support access must be disabled at the Frame Customer entity level by the Covered Entity. Frame Support personnel will then be restricted from accessing any of the accounts, their configurations, activity logs/reports, virtualized desktops/applications, or data within the Covered Entity's Frame-managed infrastructure.

- Application icons and background images may not contain any protected health information.
- Covered Entities may not use the Persistent Desktop feature or Frame Utility Servers to store PHI.

> Note on ePHI Data Storage and Processing:
> Covered Entities may not store or process ePHI on Frame-owned or managed infrastructure.

Customer Requirements

As with all cloud services, there is a shared responsibility between cloud service providers and end customers. To support HIPAA requirements, customers (Covered Entities) are responsible for the following:

- Policy controls and HIPAA compliance of their environment and workloads.
- Utilize Frame's Bring Your Own (BYO) infrastructure capabilities with either:
  - On-premises Nutanix AHV infrastructure or
  - A public IaaS provider cloud account (Covered Entity must enter into a Business Associate Agreement with their IaaS provider)
- Monitor their DaaS workloads and supporting network infrastructure.
- Ensure the security of their own DaaS workload configurations.
- Security and monitoring of their own IaaS provider configurations.
- Implement user authentication and authorization *prior* to enabling user access to HIPAA data/PHI via Frame.
- Configure Frame workloads and supporting infrastructure to meet availability requirements.
- Implement all technical and administrative controls necessary to govern access to ePHI data.
- Collect and retain audit logs for ePHI access.
- Restrict cloud credentials provided to Frame to ensure Frame does not have access to ePHI data.
- Enter into a Business Associate Agreement (BAA) with Frame.

BAA Scope

Frame will only enter BAAs scoped to our cloud service and supporting infrastructure. The scope of these Business Associate Agreements will not include the customer DaaS workload environments. Covered Entities are responsible for independently entering into a BAA with their

cloud or data center service providers that host their DaaS workloads. Please reference the links below for more information about BAAs with currently supported cloud providers:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

[^1]: A "Covered Entity" is a "Health Care Plan, Health Care Provider, or Healthcare Clearing House". Please note that Business Associates may also have downstream Business Associates who would need to comply with these requirements, (e.g., AWS as the platform hosting a SaaS application).

Refer to https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html for the definition of protected health information.

Revision #3
Created 1 October 2025 04:55:12
Updated 19 January 2026 14:38:05 by Dominik Conrad