OMNISCIENT

HIPAA Readiness & Shared Responsibility Statement

A technical and operational overview of the safeguards Omniscient provides for remote service support in healthcare and hospital environments — and the responsibilities customers retain.

Purpose

Omniscient is designed to help field technicians and remote specialists collaborate during service events while minimizing unnecessary capture, retention, and access to sensitive information. In healthcare environments, a technician's live point-of-view video may inadvertently capture protected health information (PHI) or electronic protected health information (ePHI), such as patient names, charts, worklists, monitor screens, wristbands, labels, images, or conversations.

Omniscient includes technical and administrative controls intended to support HIPAA-conscious workflows. HIPAA compliance is a shared responsibility between Omniscient and the customer. No software control can fully prevent incidental PHI exposure if a technician points an enabled camera at sensitive information. Customers must combine Omniscient's controls with appropriate HIPAA training, site procedures, access management, and incident-response processes.

> **IMPORTANT**
>
> Omniscient should not be described as "HIPAA certified" or "HIPAA approved." HIPAA does not provide a product certification program. Production workflows that intentionally involve ePHI require the appropriate contractual, operational, and technical review, including a Business Associate Agreement (BAA) where applicable.

Azure Hosting & Platform Safeguards

Omniscient's target hosted deployment runs on Microsoft Azure. The current Azure infrastructure and application design include the following safeguards:

- **Azure App Service hosting** for the API and expert dashboard, configured for HTTPS-only access, TLS 1.2 minimum, disabled FTPS, health checks, and a system-assigned managed identity.
- **Azure SQL Database** for tenant, user, session, chat, and media metadata, using encrypted connections and Microsoft Entra-only administrator authentication.
- **Azure Blob Storage** for captured media bytes, configured for HTTPS-only traffic, TLS 1.2 minimum, anonymous blob access disabled, and private media containers.
- **Managed identity access** from the application to Azure SQL and Blob Storage, avoiding storage account keys or database passwords in application code.
- **Private blob access by default.** Stored media is not anonymously public. Recording upload and playback use scoped, short-lived SAS URLs where applicable.

Current hosting does not claim private networking or isolated per-customer infrastructure by default. Azure SQL public network access and Azure-service firewall access may be enabled depending on the deployment. Additional controls such as private endpoints, customer-managed keys, dedicated storage accounts, or stricter network isolation can be evaluated for specific customer requirements.

Identity, MFA & Authorization

Omniscient supports Microsoft Entra ID based authentication for production deployments. Application authorization is role-based and tenant-aware:

- Supported application roles include **Technician**, **Specialist**, **Admin**, and **PlatformAdmin**.
- Tenant membership and application roles are resolved server-side from Omniscient's database. Tenant and role values supplied by clients are not trusted as the source of authority.
- API, dashboard, SignalR, media, and history access are protected by role and tenant checks when production authentication is enabled.
- Browser dashboard sessions use secure, HTTP-only, SameSite Lax cookies with a limited session lifetime. Lax is required for the Microsoft Entra OIDC callback; state-changing browser requests additionally require antiforgery or same-origin validation. OIDC tokens are not copied into the application cookie.

Multifactor authentication (MFA) is enforced through the customer's or hosting tenant's Microsoft Entra Conditional Access policies. Customers should require MFA for specialists, administrators, and any other users who can access call history, chat, media, or tenant administration.

Tenant Isolation

Omniscient is built as a tenant-scoped application. Business records are associated with a customer tenant, including users, memberships, subjects, sessions, chat messages, media metadata, and tenant settings. Server-side tenant resolution is used before protected operations run.

The SQL data model includes tenant identifiers on business records and is designed to use SQL Row-Level Security for tenant isolation. Blob media paths are also tenant-partitioned using a path structure such as:

TENANT-PARTITIONED MEDIA PATH

```
{tenantId}/{sessionId}/{assetId}.{extension}
```

This structure supports tenant-scoped authorization, media lookup, lifecycle management, and future tenant export or deletion workflows.

Encryption & Secure Transport

Omniscient uses encrypted transport between application boundaries:

- Technician app, expert dashboard, API, and SignalR communication use HTTPS/TLS in hosted deployments.
- WebRTC signaling is relayed through the authenticated SignalR hub.
- API-to-database communication uses encrypted Azure SQL connections.

- API-to-storage communication uses Azure Blob Storage HTTPS endpoints and managed identity.
- Stored media is accessed through private blob containers and scoped URLs rather than anonymous public links.

Live audio and video are treated separately from retained media. Live media is transient unless a photo is captured or a recording is explicitly started, uploaded, and committed.

Live Video, Mute & Video Pause Controls

The technician app provides controls intended to reduce incidental exposure:

- The technician can **mute** the microphone during a call.
- The technician can **pause video** or use a video blackout workflow without ending the call.
- The specialist cannot remotely resume the technician's video.
- When technician video is paused, photo capture and recording requests are unavailable.
- Pausing video notifies the specialist that the video stream has been paused.

Customers should instruct technicians to pause video before entering hallways, patient areas, control rooms, or any location where PHI may be visible, and to resume only when the camera is focused on the equipment or work area appropriate for the support session.

Photo, Recording & Chat Controls

Omniscient includes tenant or organization policy controls for media and chat behavior:

- Photo capture can be enabled or disabled by policy.
- Recording can be enabled or disabled by policy.
- Chat-history persistence can be enabled or disabled by policy.
- Media retention can be configured with a retention-day policy.
- Video quality and frame-rate policy can be configured for a tenant.

Photo and recording permissions are enforced by the service, not only hidden in the user interface. A specialist can request a photo or recording only when the corresponding policy permits it and the technician's video is not paused.

Recording is not automatic. It is command-driven: a specialist requests recording, the technician app records locally where supported, and the completed file is uploaded directly to Blob Storage using a short-lived write URL. Recording bytes do not traverse the SignalR hub or the API during upload.

Chat messages and typed specialist instructions are part of the support workflow. Customers should avoid entering patient names, medical record numbers, dates of birth, clinical notes, or other PHI into chat, call subjects, equipment descriptions, or diagnostic logs.

Data Retention & Storage

Omniscient retains only data created or uploaded through the support workflow. Current behavior is:

Data Type	Current Retention Behavior
Session metadata	Created sessions retain tenant, reference code, technician/specialist labels or user IDs when available, subject/procedure label, status, created time, answered time, ended time, and duration/queue timing fields.
Chat messages	Retained when chat-history persistence is enabled. The default policy enables chat-history persistence.
Photos	Retained only when photo capture is allowed and a technician uploads a captured still.
Recordings	Retained only when recording is allowed, explicitly requested, completed, uploaded, and committed. Recording is not automatic.
Diagnostics	Retained only if the technician uploads a diagnostic log for a session. Diagnostic logs are plain text and may contain device or application troubleshooting information.
Live video / audio	Not retained by default. Live media is transient unless photo capture or recording is used.
Media metadata	Retained in SQL for captured photos and recordings, including asset type, path, content type, size where available, capture time, retention deadline, and deletion timestamp where applicable.

Captured photos and recordings receive a server-decided retention deadline when the tenant policy specifies one. The default media retention policy is 30 days. A background retention service deletes expired media bytes and marks the media metadata as deleted. Metadata may be retained for audit, history, and operational purposes.

Auditability & Operational Visibility

Omniscient records operational information needed to support history, troubleshooting, and access review. This includes session status, timing, resolved user identity where available, role-based access decisions, chat history when enabled, media metadata, and diagnostic uploads when provided.

Application logs are used for operational monitoring and troubleshooting. Customers should avoid placing PHI in free-text fields because chat messages, subject labels, diagnostics, and other support data may be retained according to the configured policy.

Customer Responsibilities

Customers remain responsible for the operational safeguards required for HIPAA-compliant use, including:

1. Training technicians, specialists, and administrators on HIPAA awareness and minimum-necessary use of live video, chat, photos, recordings, and diagnostic logs.
2. Defining when wearable-camera video is permitted in hospitals, clinical spaces, control rooms, and other sensitive locations.
3. Instructing technicians not to aim the camera at patients, charts, worklists, monitor screens, wristbands, labels, records, or conversations involving PHI.
4. Requiring technicians to use mute and video pause/blackout controls when entering areas where PHI may be visible or audible.
5. Managing user onboarding, role assignment, offboarding, MFA, Conditional Access, device management, endpoint security, and screen-lock policies.
6. Confirming that hospital or site policies permit wearable-camera use for the intended service workflow.
7. Promptly reporting suspected privacy or security incidents through the agreed support process.

Summary

Omniscient provides controls that help reduce unnecessary PHI exposure and retention during remote service support. These controls include Microsoft Entra based identity, role-based authorization, tenant scoping, encrypted Azure-hosted services, managed identity access to storage and database resources, private media storage, configurable photo/recording/chat policies, retention controls, and technician-operated mute and video pause.

> These controls do not eliminate the customer's responsibility to train users and govern field procedures. A technician can still inadvertently view PHI while live video is enabled. HIPAA-ready operation requires both Omniscient's technical safeguards and the customer's administrative, physical, and operational safeguards.