## Data Security and Compliance

EVERSANA adheres to HIPAA compliance by implementing rigorous administrative, technical, and physical safeguards to protect electronic protected health information (ePHI). Our approach ensures theconfidentiality, integrity, and availability of client data at all times.

### 1. Administrative Safeguards

* **Role-Based Access Control (RBAC):** Only authorized personnel can access ePHI based on job responsibilities.
* **HIPAA Training:** All employees handling sensitive data undergo mandatory HIPAA compliance training.
* **Risk Assessments:** Regular HIPAA risk assessments are conducted to identify vulnerabilities and mitigate risks.
* **Incident Response Plan:** A formal plan is in place to respond to data breaches, including containment, impact assessment, and regulatory reporting.

### 2. Technical Safeguards

**Data Encryption:**

* **In Transit:** All data is encrypted usingTLS 1.2/1.3 for secure transmission.
* **At Rest:** Stored data is encrypted using AES-256 to prevent unauthorized access.

**Audit Logs & Monitoring:**

* All access and modifications to ePHI are logged and monitored for suspicious activity.
* Regular log reviews ensure compliance and detect potential breaches.

**Access Controls:**

* Multi-factor authentication (MFA) is enforced for system access.
* Automatic session timeouts reduce the risk of unauthorized access.

### 3. Physical Safeguards

**Data Center Security:**

* Servers hosting ePHI are located in secure, HIPAA-compliant data centers with restricted access.
* Physical security measures include biometric access controls, surveillance, and 24/7 monitoring.

**Device Security:**

* Strict policies for device encryption, remote wiping, and secure access for any workstations handling ePHI.
* Prohibition of unauthorized storage or access on personal devices.

### 4. Vendor & Third-Party Risk Management

**Business Associate Agreements (BAAs):**

* All third-party vendors processing ePHI sign BAAs, ensuring they comply with HIPAA regulations.

**Third-Party Security Audits:**

* Regular security assessments of vendors handling client data.

## Data Segmentation and Client Isolation

EVERSANA uses a multi-tenant architecture in our Snowflake data warehouse, enabling us to efficiently manage and process data for multiple clients within a shared environment. However, strict role-based access control (RBAC) and row access policies are implemented to ensure that each client’s data remains completely isolated and inaccessible to unauthorized users.

### Client Data Isolation Strategies

**Role-Based Access Control (RBAC):**

* Each client is assigned specific roles with predefined access permissions.
* Users can only access the data and resources granted to their role, ensuring strict data segmentation.
* Administrative roles are restricted to necessary functions only, minimizing access to sensitive data.

**Row Access Policies (RAPs):**

* Dynamic row-level security ensures that users can only query data belonging to their organization.
* Policies filter records **a**t query time based on the user’s assigned role.
* Prevents accidental or unauthorized cross-client data access.

**Column-Level Security:**

* Sensitive fields (e.g., PII, financial data) are masked or restricted at the column level.
* Dynamic Data Masking (DDM) in Snowflake is a powerful security feature used to protect sensitive data by controlling access at the column level. It ensures that users with different roles see different representations of the data based on their privileges—either masked or unmasked—without changing the actual data.
* At EVERSANA we often need to control access to patient’s sensitive information such as patient name, date of birth, zip etc. With dynamic data masking, we can:  
   - Mask data for general users.  
   - Show full data for privileged users (e.g., Admin, Compliance).  
   - Apply logic-based masking conditions.

**Data Encryption:**

* Data is encrypted at rest (AES-256) and in transit (TLS 1.2/1.3) to prevent unauthorized access.
* Snowflake’s key pair rotation enhances data protection.

**Regular Role Audits & Validation:**

* All roles are routinely audited to confirm they return only the data they are authorized to access. Audits include:
  + Reviewing role permissions against current business requirements.
  + Running controlled test queries to validate that sensitive data is not exposed incorrectly.
  + Logging and monitoring any unauthorized access attempts.

## Data Processing & Usage

EVESANA ingests client data primarily through secure SFTP transfers, ensuring a controlled and encrypted pipeline for data collection. Once ingested, an Extract, Load, and Transform (ELT) approach is followed to process and structure the data efficiently. Our goal is to standardize data formats across different sources while ensuring strict access controls and data minimization principles.

### Key Data Processing Practices:

**Standardized data transformation:**

* Incoming data is transformed into consistent table structures with standardized columns.
* Structured target lists and engagement data are maintained across different marketing channels.
* Original raw data is preserved but is never directly accessed by applications.

**Presentation views for controlled access:**

* Instead of exposing raw tables, filtered, task-specific secure presentation views are created.
* Views ensure applications retrieve only the minimum data necessary for their function.
* This approach enhances security, reduces data exposure risk, and simplifies compliance.

**Role-based access with No-PHI roles:**

* No-PHI roles are enforced that either:
  + Exclude electronic protected health information (ePHI)
  + Obfuscate ePHI using tokenization or data masking.
* This ensures that non-essential users and applications never access sensitive data.