SonomedEscalon™

PHI PRIVACY AND SUPPORT COMMITMENT

Our Role as Your Partner

When we provide remote support or clinical training for our medical devices, our specialists may occasionally see protected health information (PHI) on your screen. Under HIPAA, for instance, this makes us a Business Associate. This summary statement and the Default Global Data Processing and Business Associate Agreement shown below serves as our formal commitment to protecting that data and ensuring your facility remains compliant.

How We Protect Your Data

We treat your patients' data with the same level of security we use for our own corporate assets:

- Encrypted Connections: All remote support sessions use industry-standard encryption (AES-256) to ensure data cannot be intercepted.
- Access Control: Only our clients can initiate a remote support session or export of data from their systems (we do not maintain unattended access). Additionally, we use Multi-Factor Authentication (MFA) to ensure only authorized support staff can access our tools.
- Trained Specialists: Every member of our team undergoes regular data privacy training to stay current on privacy best practices.
- No Unnecessary Storage: We do not record or store patient data during support sessions unless specifically requested by you for troubleshooting, in which case it is deleted as soon as the issue is resolved.

.

Our Legal Promises

Unless we have a separate signed agreement with your facility, the Default Global Data Processing and Business Associate Agreement (BAA) shown below applies to our support services, which includes:

- Permitted Use: We will only use or see patient data to the extent necessary to provide the technical support or training you requested.
- Safeguards: We will use appropriate administrative, physical, and technical safeguards to prevent any unauthorized use or disclosure of that data.
- Reporting: In the unlikely event of a data breach on our end, we will notify your facility immediately so you can meet your reporting obligations.
- Subcontractors: If we use any third-party tools to help us, we ensure they are also bound by these same strict privacy rules.
- Return or Destruction: Once our partnership ends, we will securely destroy or return any patient data we may have in our possession.

Your Responsibility

By requesting support or training and allowing our specialists to view your screen, you are authorizing this "incidental access" under these protected terms. You are responsible for ensuring that only the necessary information is visible during our session.

Questions About Our Privacy Policy

Please contact us if you have any questions about PHI privacy policy or concerns about the way Sonomed Escalon protects PHI.

DEAULT GLOBAL DATA PROCESSING AND BUSINESS ASSOCIATE AGREEMENT (BAA)

Scope and Applicability

This Agreement applies to all services provided by Sonomed Escalon where we may access, receive, or maintain "Protected Health Information" (under HIPAA), "Medical Information" (under CMIA), or "Personal Data" relating to health (under GDPR). This agreement acts as a Business Associate Agreement (BAA) and a Data Processing Agreement (DPA).

Permitted Uses and Disclosures

We will only process, use, or disclose protected information:

- To perform the specific technical support, troubleshooting, or training requested by you.
- As strictly required by law.
- Minimum Necessary Standard: We will only access the minimum amount of data required to resolve your specific technical issue.

Core Compliance Commitments

We agree to the following "Triple-Threat" protections:

- Administrative & Technical Safeguards (HIPAA/CMIA): We maintain a formal security program, including AES-256 encryption for data in transit and at rest, and Multi-Factor Authentication (MFA) for all support staff.
- Duty of Confidentiality (CMIA): All Sonomed Escalon personnel are bound by strict, written confidentiality agreements. We will not share, sell, or disclose medical information except as explicitly authorized in this agreement.
- Data Subject Rights (GDPR/CMIA): We will assist you in responding to any patient requests to access, correct, or (where applicable under GDPR) delete their personal data.
- Subprocessor Flow-Down: Any third party we use (e.g., secure cloud storage) is contractually bound to these same privacy and security standards.

Breach Notification

To satisfy the strictest requirement (GDPR/CMIA), we will notify you of any "Security Incident" or "Breach" involving your data without undue delay, and in no event later than 72 hours after becoming aware of the incident. We will provide reasonable assistance for your own reporting obligations to the OCR, California Attorney General, or EU Data Protection Authorities.

Data Return and Destruction

Upon completion of the support ticket or termination of our services, we will securely destroy or return all copies of patient files in our possession, unless retention is required by medical device regulatory laws (e.g., FDA/MDR quality logs).

CMIA-Specific Authorization

By requesting support and allowing our representatives to access your systems, you provide "Valid Authorization" under CMIA for Sonomed Escalon to perform the necessary troubleshooting, provided we adhere to the safeguards listed herein.

Governing Law

This privacy policy forms part of our website Terms and Conditions and as such shall be governed by and construed in accordance with the laws of the State of Pennsylvania.

rev 2026-0420