Security Transparency and Labeling (Levo Gen2)

Rev	Date	Description of Change	Author

1. Contents

2. Purpose

This document serves to provide traceability to transparency and labeling information recommended for the Levo Gen 2 Tinnitus Therapy System (hereafter referred to as Levo Gen2) to be provided in premarket submissions for medical devices regarding cybersecurity in *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (FDA, 2025).

3. Scope

Table 2 below provides cybersecurity transparency information that will be accessible to the user.

The column “Guidance Recommendations” provides traceability to the FDA’s recommendations for cybersecurity labelling as they appear in *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (FDA, 2025).

The column “Labeling Information” provides users with an explanation of recommended labeling information corresponding to each item in the "Guidance Recommendations” column.

The column “MDS2 Question ID” provides users with traceability to the corresponding labeling information in the MDS2, which is available to users.

Table 2, as well as the MDS2 (**RM-215 Rev 1.0 Manufacturer Disclosure Statement for Medical Device Security (Levo Gen2)**) will be available to users through Levo’s website (https://www.levomedical.com/MDS2/) and updated as needed.

Both **LB-100 Rev 1.0 User Manual (Levo Gen2)** and **LB-101 Rev 1.0 Provider Manual (Levo Gen2)** provide information for users to access the transparency and labeling information identified in this document, as well as information for accessing the SBOM, MDS2 and Coordinated Vulnerability Disclosure process. Users are directed in both **LB-100 Rev 1.0 User Manual (Levo Gen2)** and **LB-101 Rev 1.0 Provider Manual (Levo Gen2)** to the following links:

https://www.levomedical.com/CVD/

https://www.levomedical.com/MDS2/

https://www.levomedical.com/SBOM/

4. References

4.1 Internal Documents

LB-100 Rev 1.0 User Manual (Levo Gen2)

LB-101 Rev 1.0 Provider Manual (Levo Gen2)

RM-215 Rev 1.0 Manufacturer Disclosure Statement for Medical Device Security (Levo Gen2)

4.2 External References

Table 1. External References

Doc #/Version	Description
FDA Issued: June 2025	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

5. Abbreviations and Definitions

- EOS: End of Service
- DFD: Data Flow Diagram
- HCP: Healthcare Professional
- IFU: Instructions for Use
- IT: Information Technology
- MDS2: Manufacturer Disclosure Statement for Medical Device Security
- SBOM: Software Bill of Materials

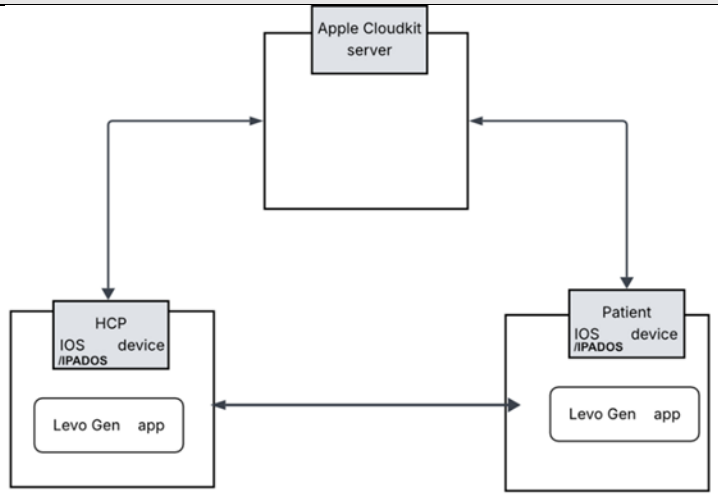
6. Traceability to Transparency and Labeling

Table 2 below provides traceability matrix referencing the following documents:

- **LB-100 Rev 1.0 User Manual (Levo Gen2)**
- **RM-215 Rev 1.0 Manufacturer Disclosure Statement for Medical Device Security (Levo Gen2)**

Table 2. Traceability to Transparency and Labeling

Guidance Recommendation	Labeling Information	MDS2 Question ID
Device instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-malware software, use of a firewall, password requirements).	Use the app only on non-jailbroken iPhone/iPad running the supported iOS/iPadOS 26 or later; keep iOS/iPadOS and the app updated via the App Store (enable automatic updates). Sign-in is required; role-based access limits what each user can view or change. Protect the device with a passcode/Face ID/Touch ID and enable auto-lock; if the device is left unattended, lock it immediately. Connectivity: the app requires outbound HTTPS to Apple services/CloudKit; no inbound ports are used. Anti-malware: do not install third-party anti-malware on iOS/iPadOS; protections rely on Apple code-signing, sandboxing, and App Store distribution. *Rationale:* App uses TLS-encrypted communications, Apple authentication, and iOS/iPadOS sandboxing/code-signing; updates are delivered via App Store	**Authentication & roles:** AUTH-1, AUTH-2, AUTH-4, AUTH-5 **Session/auto-lock:** ALOF-1, ALOF-2 **Updates/patching:** CSUP-1, CSUP-2.x **Network/ports & firewall posture:** CONN-2, NAUT-2/NAUT-3 **Anti-malware posture** (iOS/iPadOS)**:** MLDP-1, MLDP-2.x

Guidance Recommendation	Labeling Information	MDS2 Question ID
Sufficiently detailed diagrams for users that allow recommended cybersecurity controls to be implemented.		CONN-1, CONN-2, CONN-4, CONN-5, CONN-6, CONN-7 (network capabilities, ports/protocols, TLS, internet requirement) NAUT-1, NAUT-3 (node/cert-based auth) PAUT-1, PAUT-8, PAUT-9, PAUT-11 (user auth features) AUDT-2.8 (log of network/API events)
A list of network ports and other interfaces that are expected to receive and/or send data. This list should include a description of port functionality and indicate whether the ports are incoming, outgoing, or both, along with approved destination end-points	1) **Cloud data sync:** HTTPS/TLS over **TCP 443**, **outbound only**, used by the app to synchronize records with **Apple CloudKit**. The app does **not** listen on any inbound ports. 2) **App distribution/updates:** HTTPS/TLS over **TCP 443**, **outbound only**, to **Apple App Store/TestFlight** for install and update delivery. 3) **Remote sessions (SharePlay):** Apple-managed, end-to-end encrypted FaceTime channels; device-initiated; no static inbound customer-configurable ports. 4) **Nearby sessions (MultipeerConnectivity):** Peer-to-peer over local network/Bluetooth; ephemeral, consent-based connections; no persistent listening service exposed. 5) **Bluetooth audio interface:** Standard Bluetooth link to calibrated earbuds (audio only; no ePHI transmitted over Bluetooth). **Approved destinations:** Apple-managed CloudKit and App Store/TestFlight endpoints only; the app does not communicate with third-party services. **Firewall note:** Permit **outbound TCP 443** to Apple services; no inbound firewall rules are required for normal operation	**CONN-2** (list of network ports/protocols), **CONN-4** (external communications), **CONN-5** (API calls), **CONN-6** (internet required), **CONN-7** (TLS support), plus **CONN-1.2.x** as applicable for physical interfaces (e.g., Bluetooth/USB)

Guidance Recommendation	Labeling Information	MDS2 Question ID
Specific guidance to users regarding supporting infrastructure requirements so that the device can operate as intended (e.g., minimum networking requirements, supported encryption interfaces). Where appropriate, such guidance should include technical instructions to permit secure network deployment and servicing, and instructions for users on how to respond upon detection of a cybersecurity vulnerability or incident.	Use a non-jailbroken iPhone/iPad on the supported iOS/iPadOS version (26+); keep iOS/iPadOS and the app updated via the App Store/TestFlight. **Network requirement:** Internet access for CloudKit sync and updates; device initiates **outbound** connections only; no inbound listening services needed. **Encryption in transit:** Communications to CloudKit/App Store use Apple-managed TLS-encrypted channels. **Wi-Fi/cellular:** Use trusted networks when possible; the app can operate on public/unmanaged networks but relies on TLS and platform security. **Bluetooth:** Standard Bluetooth link for audio; no ePHI is exchanged over Bluetooth. (Connectivity to earbuds is shown in the comms map.) **User hardening:** Require device passcode/Face ID/Touch ID; enable auto-lock; avoid sharing accounts. **If your device is lost, stolen, or you suspect it has been compromised** • **Act immediately:** Use Apple **Find My** to **lock** the device or **erase it remotely**. • **Protect your accounts: Change your Apple ID password** (and enable/confirm **two-factor authentication**) and update any **app sign-in credentials** if applicable. • **Notify your clinic:** Contact your clinic's **support contact** as soon as possible so they can document the incident and advise next steps. **If there is a network or service outage** • **Therapy is not interrupted:** Therapy can continue **offline** using **encrypted data stored on the device**.	**CONN-1, CONN-2, CONN-4, CONN-6, CONN-7** (network capabilities, ports/protocols, internet/TLS) **PAUT-1/2/9, NAUT-1/3** (authentication/roles) **ALOF-1** (auto-lock/timeout) • **CSUP-1/2/5** (updates/patching posture) **DOC-9**(vulnerability disclosure/notification) **AUDT-2.x** (event/logging to support incident handling).

Guidance Recommendation	Labeling Information	MDS2 Question ID
	• **Sync resumes automatically:** Once connectivity returns, the app will **synchronize** normally again.	
An SBOM as specified in Section V.A.4. or in accordance with an industry accepted format to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the medical device system, and to deploy countermeasures to maintain the device's safety and effectiveness. Manufacturers should provide or make available SBOM information to users on a continuous basis. If an online portal is used, manufacturers should ensure that users have up-to-date links that contain accurate information. The SBOM should be in a machine-readable format.	The device's SBOM is provided in **machine-readable CycloneDX JSON (v1.4)** and is **continuously maintained**. SBOM can be found here: https://www.levomedical.com/SBOM/ The entries include component name/version and **maintenance status / end-of-support** fields. Contact for **coordinated vulnerability disclosure** and instructions for subscribing to notifications can be found here: https://www.levomedical.com/CVD/	**DOC-9** (vulnerability disclosure / notifications), **CSUP-1 / CSUP-2 / CSUP-5** (update/patch posture; third-party component updates), **RDMP-3 / RDMP-4** (support & end-of-life planning).
A description of systematic procedures for users to download version-identifiable manufacturer-authorized software and firmware, including a description of how users will know when software is available.	**Only install manufacturer-authorized builds** from **Apple App Store or TestFlight**; sideloading is not supported. Releases are distributed and updated via Apple's channels. **Version-identifiable releases:** App versions are managed in **Apple Store Connect** and delivered by the **App Store/TestFlight update service** (each release shows version/build). **How you'll know an update is available:** Users receive **App Store/TestFlight notifications**; the manufacturer also **notifies when**	**CSUP-2.1** (documentation of install/update steps), **CSUP-2.3** (remote installation capability), **CSUP-3** (firmware—N/A), **CSUP-7** (manufacturer notifies when updates are approved), **CSUP-8** (automatic installation), **DOC-9** (customer notifications/communications).

Guidance Recommendation	Labeling Information	MDS2 Question ID
	updates are approved; automatic installation can be enabled per Apple settings. **Step-by-step procedure:** (a) Open App Store → Search "Levo Gen2" → Install/Update; or (b) Accept TestFlight invite → Install/Update. The device downloads updates **remotely**; no onsite service is needed. **Firmware note:** This product is an iOS/iPadOS application (no device firmware); firmware update steps are **N/A**. Distribution/updates are handled through Apple's services as shown in the system DFD.	
A description of how the design enables the device to respond when anomalous conditions are detected (i.e., security events). This should include notification to the user and logging of relevant information. Security event types could be configuration changes, network anomalies, login attempts, or anomalous traffic (e.g., send requests to unknown entities).	**Authentication events (Apple ID):** The app relies on **Sign in with Apple / iCloud account state**; no app-specific usernames or passwords exist. When Apple services report **successful sign-in**, **failed/denied sign-in**, or **account/token revocation**, the app displays an in-app notice (banner + details) and records an audit entry. **Account state changes:** If the device is **signed out of iCloud**, has **restricted iCloud/CloudKit**, or the Apple ID session expires, the app shows a blocking prompt with steps to restore access (open Settings → sign in to Apple ID / enable iCloud; retry). **Configuration changes:** Changes to therapy parameters or **role/permission** assignments trigger a confirmation dialog and are written to the audit history. **Network anomalies:** Loss of connectivity, TLS/certificate errors, or rate-limits produce sync warnings; the app halts sync until secure connectivity resumes. The app uses only Apple-managed endpoints and **does not accept inbound connections**; "unknown endpoint" traffic is blocked by design.	AUDT-2 AUDT-2.1 / AUDT-2.2 AUDT-2.3 AUDT-2.6 AUDT-2.8 TXCF-3 CONN-7 (TLS support) and/or TXCF-2 (PII encrypted prior to transmission).
A high-level description of the device features that protect critical functionality (e.g., backup mode, disabling ports/communications).	**Therapy continuity (offline "backup" mode).** If internet or CloudKit are unavailable, the app continues to operate offline using the locally stored, encrypted Core Data cache so calibrated therapy and patient data remain available until sync resumes.. **Minimal attack surface for communications.** The app exposes no inbound services; communications are outbound-only via Apple-managed, encrypted channels or OS-managed MultipeerConnectivity. Receiving	DTBK-5; SAHD-7; SAHD-8; SAHD-9; CONN-3; CONN-4; CONN-7; TXCF-3; TXIG-1; NAUT-3; PAUT-1; RMOT-1.

Guidance Recommendation	Labeling Information	MDS2 Question ID
	inbound streams/resources is explicitly not supported in code, reducing exposure. **Integrity safeguards protecting the audio engine and configurations.** iOS/iPadOS code-signing and jailbreak detection prevent tampering and block execution on compromised devices, protecting therapy parameters and core functionality. **Secure decommissioning if a device is lost/stolen.** Access can be revoked in CloudKit and devices can be remotely wiped via iCloud's Find My, helping preserve safety and availability of the overall system.	
A description of backup and restore features and procedures to restore authenticated configurations.	**"Backup & Restore of Authenticated Configurations"** **What is backed up:** Therapy configurations, session records and assignments are stored in the **CloudKit container** and synchronized across authorized devices; each device also keeps an encrypted **local Core Data** cache for offline use **How restore works:** Install the app from the App Store/TestFlight, ensure the device is signed in with **Apple ID**, connect to the internet, and launch the app—CloudKit rehydrates records to the device. **Authenticated state & roles:** Access and role-based permissions are enforced by CloudKit during sync; clinicians can **revoke device access / remove patient assignments** in CloudKit	**DTBK-3, DTBK-4 , DTBK-5, DTBK-2,** NAUT-3
A description of methods for retention and recovery of device configuration by an authenticated authorized user.	**Retention.** Levo Gen2 stores each patient's configuration (therapy parameters, session logs, and treatment metadata) in an encrypted CloudKit database. The app also maintains an encrypted local Core Data cache so therapy can continue offline until connectivity is restored. **Authorized recovery.** Only authenticated users can recover configurations. After installing the app, the user signs in and the app synchronizes with CloudKit; cloud-sync flows restore the assigned patient profile and therapy settings to the device. (HCP mode permits authorized clinicians to view/update settings for their assigned patients.) **If a device is replaced or lost.** Install Levo Gen2 on the new device, sign in, connect to the internet, and allow the initial sync to complete; the configuration will repopulate from CloudKit. Clinicians can revoke a lost device's access and re-assign the patient in CloudKit if needed.	DTBK-5; PAUT-1; AUTH-2; NAUT-3; IGAU-1.

Guidance Recommendation	Labeling Information	MDS2 Question ID
A description of the secure configuration of shipped devices, instructions for user-configurable changes, and identification of user-configurable changes that could increase security risk for the medical device system. Secure configurations may include endpoint protections such as anti-malware, firewall/firewall rules, allow lists, deny lists, security event parameters, logging parameters, and physical security detection, and resetting of credentials, among others	**Secure-by-default configuration (as shipped):** 1) The app is code-signed and runs only on non-compromised iOS/iPadOS devices; it includes jailbreak detection and will refuse to run on compromised devices. 2) All communications with CloudKit use TLS; there are no inbound services opened by the app (device initiates outbound connections only). 3) Patient/HCP data are stored in sandboxed local databases and in CloudKit containers restricted by entitlements and digital signatures. 4) The application supports role-based access (HCP vs. Patient). 5) Data in transit are encrypted; unnecessary services/ports are not used. **User-configurable changes that increase risk (DO NOT DO):** 1) Disabling device biometric/passcode protections or attempting to bypass the app's jailbreak checks. (App is designed to block use on compromised devices.) 2) Installing unapproved certificates/proxies that intercept TLS or opening inbound services on the device/network. (App is designed for outbound TLS only; unnecessary services/ports should remain disabled.)	**SAHD-5.1 (role-based access controls)**; **SAHD-6/6.1/6.2 (account restrictions/least privilege)**; **SAHD-7/8/9/10 (disable unneeded shares/ports/services/apps)**; **SAHD-11/12 (restrict boot/unauthorized installs)**; **TXCF-2/3/4 (encrypted transmission/fixed destinations/authenticated connections)**; **STCF-1 (encryption at rest default)**; **AUTH-5 (restricted/kiosk-like operation)**; **SGUD-2 (instructions for permanent deletion)**.
Where appropriate for the intended use environment, a description of how forensic evidence is captured, including but not limited to any log files kept for a security event. Log file descriptions should include how, where, and in what format the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g., Intrusion Detection System	Forensic evidence and security event logging are handled by the Levo Gen2 system through built-in audit logging capabilities. These logs are generated and managed by the application and associated backend services; end-users and HCPs do not configure which events are recorded, nor directly access or modify the raw audit logs. The system audit functionality records at least the following security-relevant events, as documented in the MDS2: • Successful and unsuccessful login/logout attempts • Creation, modification, deletion of users and user privileges • Creation, modification, deletion of data	AUDT-1, AUDT-1.1, AUDT-2, AUDT-2.1, AUDT-2.2, AUDT-2.3, AUDT-2.4, AUDT-2.6, AUDT-2.7 (if applicable), AUDT-2.8, AUDT-2.8.1, AUDT-2.8.2, AUDT-2.10, AUDT-4.1, AUDT-5, AUDT-5.3, AUDT-5.4, AUDT-7, AUDT-7.1, AUDT-8.

Guidance Recommendation	Labeling Information	MDS2 Question ID
(IDS) or Security Information and Event Management (SIEM))	• Receipt/transmission of data or commands over network connections (including remote/on-site support and API activity) • Software update–related events The system audit functionality records at least the following security-relevant events, as documented in the MDS2: • Successful and unsuccessful login/logout attempts • Creation, modification, deletion of users and user privileges • Creation, modification, deletion of data • Receipt/transmission of data or commands over network connections (including remote/on-site support and API activity) • Software update–related events Audit logs: • Are protected against unauthorized access and modification. • Record time information (with support for synchronization to a trusted time source such as NTP or equivalent). • Are encrypted in transit and on storage media. • Can be exported via supported communications mechanisms (e.g., via the associated service/mobile application infrastructure) for analysis by the manufacturer or the operator's security team.	
Information, if known or anticipated, concerning device cybersecurity (including components) end of support and end of life. At the end of support, a manufacturer may no longer be able to reasonably provide security patches or software updates. If the device remains in service following the end of support, the manufacturer should have a pre-established and pre-communicated process for transferring the risks	**Security Support & End-of-Support (EOS) Notice"** Levo Gen2 software and its components are monitored for security support status using a maintained SBOM that records **Maintenance Status** and **End-of-Support Date** fields for each component. If, at any point, the manufacturer can no longer provide reasonable security patches or updates for Levo Gen2 (i.e., product EOS), the manufacturer will **communicate the device EOS date and related cybersecurity implications through** the same channels used for SBOM and security communications.	RDMP-3, **RDMP-4, SBOM-1–4, DOC-9**

Guidance Recommendation	Labeling Information	MDS2 Question ID
highlighting that the cybersecurity risks for end-users can be expected to increase over time.		
Information on securely decommissioning devices by sanitizing the product of sensitive, confidential, and proprietary data and software.	**"Secure Decommissioning of Devices"** **Local data characteristics.** Levo Gen2 stores patient and HCP data in the iOS/iPadOS app sandbox using encrypted local Core Data, plus synchronized records in the CloudKit container; there is **no removable media** and no hardcopy export containing PII. **Decommissioning steps for a device that will no longer be used:** 1) If possible, **sign out** the user from the app / Apple ID used for Levo Gen2. 2) **Delete the Levo Gen2 app** from the device to remove the local encrypted database from that device. 3) For clinical deployments, the authorized HCP/administrator **revokes device access and/or removes assignments in CloudKit**, so that the retired device cannot resync if it is ever reused 4) For lost or compromised devices, use **Apple's "Erase iPhone" / Find My remote wipe** to sanitize local data. **Result.** After app deletion or device wipe plus CloudKit revocation, no active copy of sensitive data remains on the retired device; authoritative records are retained in CloudKit under controlled access. (No factory-reset utility or custom media-sanitization feature is implemented beyond these platform-supported mechanisms.)	**SGUD-2** (permanent deletion instructions) **STCF-1, STCF-1.1–1.3** (encryption at rest by default) **MPII-2.3** (PII preserved until explicitly erased) **DTBK-5** (restore from backup after decommissioning if needed).