OUTCOME BASED TECHNOLOGIES
RECOVERY BUILT AROUND YOU

PRIVACY & SAFETY POLICY

Outcome-Based Technologies, LLC (“OBT”, “we”, “our”, or “us”) is committed to protecting the privacy, safety, and security of users of our websites and mobile applications, including obtdme.com, levionusa.com, and the Levion™ application (listed on the Apple App Store as “OBT 3d Scan”). This Privacy & Safety Policy explains how we collect, use, disclose, retain, and protect your information when you interact with our websites, applications, products, and services.

1. Cookie Policy

We use cookies and similar technologies to improve website functionality, analyze traffic, remember user preferences, and enhance the overall browsing experience.

Cookies are small text files stored on your device by your web browser.

You may disable cookies through your browser settings; however, certain portions of the website may not function properly if cookies are disabled.

2. Information We Collect

We may collect personal information you voluntarily provide, including your name, email address, phone number, shipping address, billing address, clinic or company information, and product-related information.

We may also automatically collect certain technical information such as IP address, browser type, device information, operating system, website activity, and general geographic region.

When a healthcare provider places an order through the OBT 3d Scan app, we also collect the patient information entered with the order (patient name, email address, phone number and, if the order ships to the patient, the patient’s shipping address) and the patient scan described in Section 8. The app asks for access to the device camera only to perform scans.

3. How We Use Information

We may use collected information to provide products and services, process transactions, respond to inquiries, improve website functionality, provide customer support, send updates or newsletters, and comply with legal obligations.

We do not sell personal information to third parties. Patient information and scans are used only as described in Section 8 and in our HIPAA & PHI Policy.

4. Sharing of Information

We may share information with trusted third-party providers that assist with website hosting, payment processing, shipping, analytics, customer support, or marketing communications. Patient information and scans are never shared for marketing purposes and are shared only as described in Section 8.

We may disclose information when required by law or when necessary to protect our rights, investigate fraud, or comply with legal processes.

5. Data Security

We implement reasonable administrative, technical, and physical safeguards designed to help protect personal information from unauthorized access, disclosure, alteration, or destruction.

No method of electronic transmission or storage is completely secure, and we cannot guarantee absolute security.

6. HIPAA & Protected Health Information (PHI)

Certain communications or transactions involving medical products may involve protected health information (“PHI”).

OBT takes reasonable measures to safeguard PHI in accordance with applicable laws and industry standards.

7. App Account Deletion & Record Retention

Deleting your app account will disable your access to the OBT/Levion™ application and may delete or deactivate account information that OBT is not required or permitted to retain.

To delete your account, open the account menu in the app and select Delete Account. OBT completes account deletion within 30 days. Deleting the app from your device also removes all scans stored on that device. Requests to delete patient scans are handled as described in Section 8.

Account deletion does not necessarily delete patient scans, order information, device specifications, manufacturing records, fitting information, or related documentation previously submitted to or generated by OBT. These records may form part of OBT’s medical device, quality management, manufacturing, transaction, or other regulated business records.

OBT may retain such records for the period required or permitted by applicable law, regulation, quality management system requirements, healthcare record-retention requirements, contractual obligations, or other legitimate legal and regulatory purposes. This may include records maintained under applicable U.S. Food and Drug Administration medical device requirements, including the Quality Management System Regulation (QMSR).

HIPAA does not itself establish a general medical-record retention period. However, to the extent retained information constitutes protected health information (“PHI”) and HIPAA applies, OBT will continue to protect that PHI in accordance with applicable privacy and security requirements for as long as the information is maintained.

By requesting deletion of an app account, you acknowledge that deletion of the account and access to the application is separate from deletion of records that OBT is required or permitted to retain. Retained records will not be deleted solely as a result of an app account deletion request and will remain subject to applicable privacy and security protections.

8. Patient Scans and Facial Image Data (OBT 3d Scan App)

What we collect. Healthcare providers use the OBT 3d Scan app to order a custom-fabricated Levion™ cervical collar. To capture the patient’s anatomy, the provider scans the patient’s neck with the device’s rear camera. The app records a series of standard color photographs of the patient’s neck area. On devices with a rear LiDAR sensor, the app also records depth maps from that sensor. Because the collar fits under the jaw, these photographs may include part of the patient’s face, such as the chin and jawline,

or the whole face or head. Patients are often scanned wearing a thin stocking over the head and neck, which obscures facial features. The photographs are processed into a three-dimensional (3D) model of the neck area and a color texture image, which may also show part of the face (together, “Scan Data”).

The app does not use Face ID, the TrueDepth camera, face tracking, face detection or facial recognition. We do not create facial templates, faceprints or any other biometric identifier from Scan Data, and we do not use Scan Data to identify or authenticate anyone.

How we use it. We use Scan Data only to design, manufacture, fit and support the patient’s custom medical device and to keep the related order, quality and regulatory records. Our scanning provider also uses depth maps to diagnose scanning problems in support of its service. We do not use Scan Data for advertising, marketing, analytics or profiling, we do not use it to develop or train machine-learning or artificial-intelligence models, and we do not sell it.

Who we share it with. We share Scan Data only with service providers that process it on our behalf to produce the device: MyFit Solutions (scanning and 3D reconstruction), Google Cloud/Firebase (app backend, which stores order status but no images or scan files), Resend (delivery of the order email to OBT), Make.com (OBT’s order automation), Microsoft 365 (OBT’s secure record storage) and HP Inc. (the developer of OBT’s collar design software, which may receive individual scans when needed to troubleshoot that software). These providers are contractually required to protect Scan Data and to use it only to provide their services to OBT. OBT is not a HIPAA covered entity. We may also disclose Scan Data as described in our HIPAA & PHI Policy, for example to the treating healthcare provider or when required by law. OBT designs and manufactures the device in-house and does not send Scan Data to other manufacturers.

Where it is stored. Scan Data is sent over encrypted connections and stored on secure servers in the United States operated by our service providers and in OBT’s record systems. MyFit’s support staff in France may access Scan Data to provide the service. Photographs captured during a scan, and scans a provider opens in the app, are also kept in the app’s private, encrypted storage on the provider’s device and are removed when the app is deleted.

How long we keep it. 3D models and order records are kept as part of OBT’s medical device and quality records for ten (10) years from the date the device is manufactured, to meet medical device and medical record retention requirements, then securely destroyed or permanently de-identified. MyFit Solutions keeps Scan Data while the provider’s account is in use and erases it automatically, photographs included, after one year without account activity. Our other service providers keep Scan Data only as long as needed to provide their services to OBT. HP Inc. deletes scans it receives for troubleshooting once the issue is resolved. Our email delivery provider keeps order emails, and our order automation provider keeps its run records, for up to 30 days. Our app backend stores no Scan Data; its order status records are deleted after 14 days, and backup copies expire within 98 days.

Deletion requests. Providers can delete their app account as described in Section 7. Patients and providers may ask us to delete Scan Data by emailing cs@obtdme.com. OBT customer service will delete Scan Data held by OBT and our service providers that we are not required to keep, within 30 days of the request. Scan Data that forms part of a manufactured device’s records is kept for the period stated above and protected as described in this Policy and our HIPAA & PHI Policy.

Patient consent. The healthcare provider performing the scan is responsible for informing the patient and obtaining any consent or authorization required for the scan, including from a parent or guardian for a minor.

9. Medical Disclaimer

Information provided on our websites is intended for general informational purposes only and does not constitute medical advice.

Our products should only be used under the direction of a licensed healthcare provider.

10. Intellectual Property

Unless otherwise stated, all website content, including text, graphics, logos, product designs, downloads, trademarks, and documentation are the property of Outcome-Based Technologies, LLC or its licensors.

Website materials may not be reproduced, republished, distributed, modified, or exploited without prior written permission.

11. Website & App Acceptable Use

You agree not to use our websites or applications in violation of applicable laws or regulations.

You must not transmit malicious software, interfere with website or application functionality, scrape data, or attempt unauthorized access to systems or accounts.

12. Limitation of Liability

To the maximum extent permitted by law, our websites and content are provided “AS IS” and “AS AVAILABLE.”

We make no warranties, express or implied, regarding the accuracy, reliability, or availability of the websites or their content.

13. Third-Party Links

Our websites may contain links to third-party websites or services. We are not responsible for the privacy practices, policies, or content of third-party websites.

14. Children’s Privacy

Our websites and applications are not intended for children under the age of 13, and we do not knowingly collect personal information from children.

Patients scanned by healthcare providers may include children. Their information is entered by the treating provider, not by the child, and is handled as described in Section 8 and our HIPAA & PHI Policy.

15. Changes to This Policy

We may update this Privacy & Safety Policy from time to time. Updated versions will be posted with a revised effective date.

16. Governing Law

This Privacy & Safety Policy shall be governed by the laws of the State of Arizona, without regard to conflict of law principles.

17. Contact Information

OUTCOME BASED TECHNOLOGIES
RECOVERY BUILT AROUND YOU

Outcome-Based Technologies, LLC
7830 E Gelding Dr, Suite 300
Scottsdale, AZ 85260
T. (888) 609-2563
F. (888) 619-5948
Email: info@obtdme.com
Website: www.obtdme.com

Effective Date: October 22, 2026