SECURITY STATEMENT

At SHOEBOX Ltd. ("**SHOEBOX**"), the security of your data is critical. The purpose of this security statement is to provide a high-level overview of our security architecture, security frameworks, data handling methods, policies, procedures, certifications, and compliance.

About SHOEBOX Products

SHOEBOX® PureTest is an iPad-based audiometer that is used in conjunction with the SHOEBOX Data Management Portal to perform diagnostic hearing testing.

SHOEBOX® Platform is an online audiological platform (consisting of **SHOEBOX® Remote** and **SHOEBOX® Consult**) intended for use in conducting hearing testing for diagnosis of possible otologic disorders.

SHOEBOX® Online is an online hearing screening test. SHOEBOX Online is not a medical device.

SHOEBOX® Data Management Portal is a cloud data storage system that is used to synchronize and store the data collected in association with the use of all SHOEBOX products. SHOEBOX Data Management Portal is not a medical device.

SHOEBOX® Audiometry Standard and SHOEBOX® Audiometry Pro are registered medical devices in certain jurisdictions. They are tablet-based audiometers that perform diagnostic hearing testing.

SHOEBOX® QuickTest is a tablet-based hearing screening test. SHOEBOX QuickTest is not a medical device.

Collectively, we refer to these products as the "**SHOEBOX Solutions**".

The products that run on iOS (iPad) are **SHOEBOX® Audiometry Standard, SHOEBOX® Audiometry Pro, and SHOEBOX® QuickTest** and are collectively referred to as **SHOEBOX Apps.**

SECURITY OVERVIEW

Legal and Regulatory Compliance

SHOEBOX maintains compliance with applicable data protection regulations, including US HIPAA regulations, Canadian privacy legislation (PIPEDA), and GDPR, with a Data Processing Agreement (DPA) in place as per Article 28 of the GDPR.

SHOEBOX Ltd is ISO 27001:2013 certified (since Oct 2021) from British Standard Institute (BSI). SHOEBOX Solutions are hosted on Amazon AWS or Heroku which are compliant with multiple standards including ISO 9001, SOC 2 Type II, ISO 27001, and HDS: https://aws.amazon.com/compliance/programs/

SHOEBOX has a signed BAA with Amazon for **HIPAA compliance**. SHOEBOX also offers a BAA to US customers of its SHOEBOX service who must comply with HIPAA. Alignment with the HIPAA requirements for Administrative 164.308, Physical 164.310, and Technical 164.312 safeguards, the Privacy Rule(s) 164.5xx, and Breach Notification (164.4xx) has been externally audited by ***HIPAA Solutions RX*** (who concluded that *"SHOEBOX had conducted one of the more **thorough and comprehensive** HIPAA Security/Privacy Risk Analysis seen over the years" and that the consultant "was unable to identify any significant risks/privacy vulnerabilities that have not been addressed by SHOEBOX").* SHOEBOX annually updates and internally audits a detailed HIPAA worksheet that cross-references our controls with our policies and procedures that are audited under ISO 27001.

Risk Assessment and Management

SHOEBOX maintains an ISO 13485 certification for its Quality Management system which includes overlapping privacy and security requirements. Risk Analysis is performed both from a **medical device** point of view (patient harm) as well as from an **information asset** point of view (patient privacy) using risk management frameworks from ISO 13485, ISO 27001, ISO 27005, and ISO 31000.

Vendor Management

We use a supplier management / vendor assessment process for all our software suppliers, cloud hosting providers, hardware providers, etc. Suppliers must be approved by our Regulatory, Finance, Legal, and Security departments. All suppliers are reviewed at least annually.

Data Collection, Transmission, and Storage

All data captured using the **SHOEBOX Apps** is stored in a segregated database that is 'firewalled' from other iPad applications. Backups to non-compliant systems, such as a personal computer, are disabled. If selected, data is automatically backed up to AWS. Data is encrypted in transit (TLS v1.2 or higher) and at rest (AES-256) once stored in the cloud.

The **SHOEBOX Apps** can be used to collect and transmit certain data to the **SHOEBOX® Cloud Storage Service** running on AWS; the nature and purpose of this is detailed within the Data Processing Addendum (DPA) on the website.

Data Residency

Data hosting location depends on the country of the customer:
- For US customers: N. Virginia AWS data center

- For rest of world customers: Canada Central (Montreal) AWS data center

Customer data and backups of that data are never exported out of the host country.

While SHOEBOX operates out of a single corporate office located in Ottawa, Canada, no customer data is ever stored on site.

Physical Security

The company has documented policies that prohibit the storage of Protected Health Information (PHI) at SHOEBOX offices or on SHOEBOX owned computers, email systems, or in any 3rd party services other than our certified production servers. Data is physically secured in Amazon's data warehouses only. These facilities are monitored and staffed 24×7 and the servers are protected in locked cages. Details of the extensive security features can be found on the AWS security page.

Data Retention

As long as your account is active, any data backed up to your cloud account will be retained until you intentionally delete it. If you cancel or do not renew your cloud subscription, you will have 60 days to download your data after which it may be permanently deleted from the system.

Access Control

By default, all SHOEBOX products authenticate users using login/password. Usernames must be an email address. Before the account can be used, the user must verify the account by clicking on a link emailed to the user.

When the user initially sets their password, we hash the password with PBKDF2 using a secure, randomly-generated salt and store the hash in our database. A password is authenticated by comparing with the hashed version of the password stored in the database. The original plaintext values are never retained.

Configurable password-complexity rules include: Minimum Length, Require Letters & Numbers, Require Upper & Lower, Special Characters, Lockout Attempts, Lockout Length, Password Reuse, & Expiration.

Passwords can be self-reset by using the *'Forgot Password'* feature on the web portal. The system will send an email to the user with a link to reset their password.

Single Sign On (SSO) authentication is available for certain customers of SHOEBOX Portal (including administration of SHOEBOX Online) and SHOEBOX Puretest if they have an existing identity provider (IdP), AND is only available if explicitly offered as a part of your onboarding. (Note that SHOEBOX Standard, Pro, & QuickTest do not support SSO).

SHOEBOX leverages Amazon Cognito to enable Single Sign On (SSO) authentication (introduced 2021-Q4) for users of SHOEBOX Portal and SHOEBOX Puretest. This adds support for SAML 2.0 and OAuth 2.0, allowing customers to authenticate users within their corporate identity provider (Azure AD, Okta, and others) empowering I.T. departments to enforce MFA and centralize the management of SHOEBOX users accounts.

Instructions to enable SSO are here:
https://help.shoebox.md/Content/SHOEBOX_Data_Management/SSO_Implementation.htm

Access to the Production Environment

SHOEBOX Solutions are designed so that no SHOEBOX employee can access customer data, except under exceptional circumstances. Software developers only have access to a separate Staging environment. Deployment of software updates to production is done via a release team that has restricted access to only update software but will not have access to production data.

Access to the production environment is protected using an authenticated VPN connection. Access also requires a second factor, one-time password (OTP) card.

Access to customer data requires a special request from the customer and with the approval of senior management.

Employee Security

All employees have been screened with criminal background checks where permitted by law. We also perform reference, qualification, and criminal record checks on all of our audiological reviewers.

Training and Awareness

All employees with access to PHI have been trained on data privacy requirements (including HIPAA, PIPEDA, and GDPR). An automated anti-phishing training program inoculates employees against social engineering campaigns.

Separation from Company Network

SHOEBOX's internal company network is entirely separate from the production network. All machine ports are locked down with security groups using a firewall, leaving only a single port available to the traffic management network. All storage uses encrypted volumes at all times.

Quality Assurance and Testing

SHOEBOX has an ISO 13485 compliant process for maintaining the quality of our software. Any code changes are tested using a combination of manual and automated regression tests. All code changes are tested in separate QA and Staging environments prior to release.

Internal and External Security Testing and Verification

SHOEBOX performs internal and external security testing to verify the integrity of our systems. Code is automatically scanned during our regular build process. Our employees are trained on standard security best practices for software development to minimize the chance of introducing vulnerabilities into our code. Our technology selection further encourages these practices. For example, SQL injection attacks are prevented by exclusive use of prepared statements for database access. In addition, we conduct regular peer reviews of code. New issues are tracked and assigned to our engineering team as part of our daily review process.

The company engages external penetration testers to validate security controls. Testing involves vulnerability testing of our network and application code.

Vulnerability Management and Patching

Our engineering team monitors security alerts from multiple sources. Alerts for security issues and patches for infrastructure are automatically generated. Security alerts are managed and prioritized in our issue tracking system. Validated issues are then assigned to our engineering team for remediation. All issues are recorded, assigned and closed in our issue management system.

Our engineering team conducts daily reviews of the backlog and issues are assigned according to priorities. Mission-critical issues are monitored daily and addressed immediately if there are implications to our production systems. We release portal and app feature updates about every 6 weeks which are always patched to include the most recent version of the operating systems and libraries used. Any critical vulnerabilities are patched as soon as available in a point-release as per our Patch Management Policy. The current product version information can be found on the SHOEBOX website: https://www.shoebox.md/software-updates/

As with all changes to production, testing (in separate QA environments) and release is controlled via our gated Design & Development process which is annually audited for compliance with ISO 13485, IEC 62034, and ISO 27001.

OS and Database Hardening

We only use Amazon-certified pre-hardened OS images to build our platform. By default, our security policies state that all ports be closed, and then only opened to the minimum required to provide access to our services.

System Monitoring and Logging

Amazon Cloudwatch monitors the health of our systems. We also use a flexible and scalable system to centralize access logs, and we monitor those logs to look for suspicious activity. Logging covers all authentication attempts, as well as all create, update, delete, and view requests of patient data.

Incident Response, Incident Reporting and Breach Notification

Our incident response, communication, and reporting policies and procedures are established in alignment with the ISO 27001 and ISO 13485 standards. Our incident response systems are exercised regularly.

In the unlikely event of a breach, per the Data Processing Addendum (DPA), we commit to notifying customers who are affected within 72 hours of discovery.

As a data processor, our primary commitment under the DPA is to support and assist you, the data controller, in fulfilling your obligations under the GDPR, including Articles 33 and 34. In the event of a personal data breach, we will promptly notify you without undue delay, providing all relevant information to facilitate your notification to the supervisory authority as required by Article 33. We will also cooperate fully with you in fulfilling your obligations under Article 34, providing any necessary assistance and information to enable you to notify affected individuals if a breach is likely to result in a high risk to their rights and freedoms.

Business Continuity

At SHOEBOX, formal BC/DR tabletop exercises or simulation scenarios are scheduled quarterly.

Both SHOEBOX and Amazon have defined Emergency mode and Disaster recovery procedures designed to ensure business continuity in any situation.

Data Backups

Our backup system operates as follows:

- All data in the **SHOEBOX® Data Management Portal** is backed up daily.
- Daily backups are stored for 1 year.
- The database journal (incremental data changes) is backed up in real time.
- Database backups are stored on Amazon S3 and can be recovered in 6 hours.
- Data in the storage service, S3, is redundant with 3 copies of data in different physical locations.

Our backup strategy protects against irreversible database corruption.

System Availability and Redundancy

Our solution automatically scales resources based on load and balances across physically separated data centers.

Scheduled Downtime

Our system has been designed for 100% availability, however, if scheduled downtime is required, we will provide at least 48 hours prior notice. Scheduled downtime (in addition to real-time service status) is posted at https://www.shoebox.md/status

Technical Support

Telephone and email support are available from 8am - 8pm Eastern Standard Time via https://www.shoebox.md/support