DÉCLARATION DE SÉCURITÉ

Chez SHOEBOX Ltd. (« **SHOEBOX** »), la sécurité de vos données est primordiale. L'objectif de cette déclaration de sécurité est de fournir un aperçu général de notre architecture de sécurité, de nos cadres de sécurité, de nos méthodes de traitement des données, de nos politiques, procédures, certifications et conformité.

À propos des produits SHOEBOX

SHOEBOX® PureTest est un audiomètre sur iPad utilisé conjointement avec le portail de gestion des données SHOEBOX pour effectuer des tests auditifs diagnostiques. SHOEBOX PureTest est un dispositif médical.

SHOEBOX® QuickTest est un test de dépistage auditif sur tablette. SHOEBOX QuickTest n'est pas un dispositif médical.

SHOEBOX® Online est un test de dépistage auditif en ligne. SHOEBOX Online n'est pas un dispositif médical.

Portail de gestion des données SHOEBOX® est un système de stockage de données en nuage utilisé pour synchroniser et stocker les données collectées dans le cadre de l'utilisation de tous les produits SHOEBOX. Le portail de gestion des données SHOEBOX n'est pas un dispositif médical.

Collectivement, nous désignons ces produits sous le nom de « **Les solutions SHOEBOX** ».

Les produits fonctionnant sous iOS (iPad) sont **SHOEBOX® PureTest** et **SHOEBOX® QuickTest** et sont collectivement désignés sous le nom de **SHOEBOX Apps.**

APERÇU DE LA SÉCURITÉ

Conformité juridique et réglementaire

SHOEBOX maintient sa conformité aux réglementations applicables en matière de protection des données, y compris les réglementations américaines HIPAA, la législation canadienne sur la protection de la vie privée (PIPEDA) et le RGPD, avec un Accord de traitement des données (DPA) en place conformément à l'article 28 du RGPD.

SHOEBOX Ltd est certifiée ISO 27001:2022 (depuis octobre 2021) par le British Standard Institute (BSI). Les solutions SHOEBOX sont hébergées sur Amazon AWS, conformes à de multiples normes dont ISO 9001, SOC 2 Type II, ISO 27001 et HDS : https://aws.amazon.com/compliance/programs/

SHOEBOX a signé un BAA avec Amazon pour la **conformité HIPAA**. SHOEBOX offre également un BAA aux clients américains de son service SHOEBOX qui doivent se conformer à la réglementation HIPAA. L'alignement sur les exigences HIPAA relatives aux mesures de protection administratives 164.308, physiques 164.310 et techniques 164.312, aux règles de confidentialité 164.5xx et aux notifications de violation (164.4xx) a été audité en interne. SHOEBOX met à jour annuellement et audite en interne un tableau HIPAA détaillé qui croise nos contrôles avec nos politiques et procédures auditées dans le cadre de l'ISO 27001.

Évaluation et gestion des risques

SHOEBOX maintient une certification ISO 13485 pour son système de gestion de la qualité qui comprend des exigences de confidentialité et de sécurité croisées. L'analyse des risques est effectuée tant du point de vue des **dispositifs médicaux** (préjudice au patient) que du point de vue des **actifs informationnels** (confidentialité du patient) en utilisant les cadres de gestion des risques ISO 13485, ISO 27001, ISO 27005 et ISO 31000.

Gestion des fournisseurs

Nous utilisons un processus de gestion des fournisseurs et d'évaluation des prestataires pour tous nos fournisseurs de logiciels, fournisseurs d'hébergement en nuage, fournisseurs de matériel, etc. Les fournisseurs doivent être approuvés par nos départements Réglementaire, Finance, Juridique et Sécurité. Tous les fournisseurs sont réévalués au moins une fois par an.

Collecte, transmission et stockage des données

Toutes les données collectées à l'aide des **SHOEBOX Apps** is stored in a segregated database that is « protégée par pare-feu » 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** peuvent être utilisées pour collecter et transmettre certaines données au **Portail de gestion des données SHOEBOX®** fonctionnant sur AWS ; la nature et l'objectif de ces données sont détaillés dans l'Addendum au traitement des données (DPA) sur le site web.

Résidence des données

L'emplacement d'hébergement des données dépend du pays du client :
- Pour les clients américains : centre de données AWS de Virginie du Nord
- Pour les clients du reste du monde : centre de données AWS Canada Central (Montréal)

Les données des clients et leurs sauvegardes ne sont jamais exportées hors du pays d'hébergement.

Bien que SHOEBOX opère à partir d'un seul siège social situé à Ottawa, Canada, aucune donnée client n'est jamais stockée sur place.

Sécurité physique

L'entreprise dispose de politiques documentées interdisant le stockage des informations de santé protégées (PHI) dans les bureaux de SHOEBOX, sur les ordinateurs de SHOEBOX, les systèmes de messagerie ou dans tout service tiers autre que nos serveurs de production certifiés. Les données sont physiquement sécurisées uniquement dans les centres de données d'Amazon. Ces installations sont surveillées et dotées de personnel 24h/24, 7j/7, et les serveurs sont protégés dans des cages verrouillées. Les détails des mesures de sécurité approfondies sont disponibles sur la page de sécurité AWS.

Conservation des données

Tant que votre compte est actif, toutes les données sauvegardées sur votre compte en nuage seront conservées jusqu'à ce que vous les supprimiez intentionnellement. Si vous résiliez ou ne renouvelez pas votre abonnement en nuage, vous disposerez de 60 jours pour télécharger vos données, après quoi elles pourront être définitivement supprimées du système.

Contrôle d'accès

Par défaut, tous les produits SHOEBOX authentifient les utilisateurs par identifiant/mot de passe. Les noms d'utilisateur doivent être une adresse courriel. Avant que le compte puisse être utilisé, l'utilisateur doit vérifier le compte en cliquant sur un lien envoyé par courriel.

Lorsque l'utilisateur définit initialement son mot de passe, nous hachons le mot de passe avec PBKDF2 en utilisant un sel aléatoire sécurisé et stockons le hachage dans notre base de données. Un mot de passe est authentifié par comparaison avec la version hachée du mot de passe stockée dans la base de données. Les valeurs en texte clair d'origine ne sont jamais conservées.

Les règles configurables de complexité des mots de passe incluent : longueur minimale, exigence de lettres et chiffres, exigence de majuscules et minuscules, caractères spéciaux, tentatives de verrouillage, durée de verrouillage, réutilisation des mots de passe et expiration.

Les mots de passe peuvent être réinitialisés en utilisant la fonction *« Mot de passe oublié »* sur le portail web. Le système enverra un courriel à l'utilisateur avec un lien pour réinitialiser son mot de passe.

L'authentification unique (SSO) est disponible pour certains clients du portail SHOEBOX (y compris l'administration de SHOEBOX Online) et SHOEBOX Puretest s'ils disposent d'un fournisseur d'identité existant (IdP), ET n'est disponible que si elle est explicitement proposée dans le cadre de votre intégration.
(Veuillez noter que SHOEBOX Standard, Pro et QuickTest ne prennent pas en charge le SSO).

SHOEBOX utilise Amazon Cognito pour permettre l'authentification unique (SSO) (introduite au T4 2021) pour les utilisateurs du portail SHOEBOX et SHOEBOX Puretest. Cela ajoute la prise en charge de SAML 2.0 et OAuth 2.0, permettant aux clients d'authentifier les utilisateurs au sein de leur fournisseur d'identité d'entreprise (Azure AD, Okta et autres), donnant aux départements informatiques la capacité d'appliquer l'AMF et de centraliser la gestion des comptes utilisateurs SHOEBOX.

Les instructions pour activer le SSO sont disponibles ici :
https://help.shoebox.md/Content/SHOEBOX_Data_Management/SSO_Implementation.htm

Accès à l'environnement de production

SHOEBOX Solutions sont conçues de sorte qu'aucun employé de SHOEBOX ne puisse accéder aux données des clients, sauf dans des circonstances exceptionnelles. Les développeurs n'ont accès qu'à un environnement de préproduction séparé. Le déploiement des mises à jour logicielles en production est effectué par une équipe de mise en production qui dispose d'un accès restreint à la seule mise à jour du logiciel et n'a pas accès aux données de production.

L'accès à l'environnement de production est protégé par une connexion VPN authentifiée. L'accès nécessite également un second facteur, une carte de mot de passe à usage unique (OTP).

L'accès aux données des clients nécessite une demande spéciale du client et l'approbation de la direction.

Sécurité des employés

Tous les employés ont fait l'objet d'une vérification des antécédents judiciaires lorsque la loi le permet. Nous effectuons également des vérifications de références, de qualifications et de casier judiciaire pour tous nos réviseurs audiologiques.

Formation et sensibilisation

Tous les employés ayant accès aux PHI ont été formés aux exigences de confidentialité des données (y compris HIPAA, PIPEDA et RGPD). Un programme automatisé de formation anti-hameçonnage protège les employés contre les campagnes d'ingénierie sociale.

Séparation du réseau d'entreprise

Le réseau interne de SHOEBOX est entièrement séparé du réseau de production. Tous les ports des machines sont verrouillés avec des groupes de sécurité utilisant un pare-feu, ne laissant qu'un seul port disponible pour le réseau de gestion du trafic. Tout le stockage utilise des volumes chiffrés en permanence.

Assurance qualité et tests

SHOEBOX dispose d'un processus conforme à la norme ISO 13485 pour maintenir la qualité de nos logiciels. Toute modification de code est testée à l'aide d'une combinaison de tests de régression manuels et automatisés. Toutes les modifications de code sont testées dans des environnements d'assurance qualité et de préproduction séparés avant la mise en production.

Tests et vérification de sécurité internes et externes

SHOEBOX effectue des tests de sécurité internes et externes pour vérifier l'intégrité de nos systèmes. Le code est automatiquement analysé lors de notre processus de compilation régulier. Nos employés sont formés aux meilleures pratiques de sécurité standard pour le développement logiciel afin de minimiser les risques d'introduction de vulnérabilités dans notre code. Notre sélection technologique encourage davantage ces pratiques. Par exemple, les attaques par injection SQL sont empêchées par l'utilisation exclusive de requêtes préparées pour l'accès aux bases de données. De plus, nous effectuons des revues de code par les pairs régulières. Les nouveaux problèmes sont suivis et assignés à notre équipe d'ingénierie dans le cadre de notre processus de revue quotidien.

L'entreprise fait appel à des testeurs de pénétration externes pour valider les contrôles de sécurité. Les tests comprennent des tests de vulnérabilité de notre réseau et de notre code applicatif.

Gestion des vulnérabilités et correctifs

Notre équipe d'ingénierie surveille les alertes de sécurité provenant de sources multiples. Les alertes pour les problèmes de sécurité et les correctifs d'infrastructure sont générés automatiquement. Les alertes de sécurité sont gérées et priorisées dans notre système de suivi des problèmes. Les problèmes validés sont ensuite assignés à notre équipe d'ingénierie pour remédiation. Tous les problèmes sont enregistrés, assignés et clôturés dans notre système de gestion des problèmes.

Notre équipe d'ingénierie effectue des revues quotidiennes du carnet de commandes et les problèmes sont assignés selon les priorités. Les problèmes critiques sont surveillés quotidiennement et traités immédiatement s'ils ont des implications sur nos systèmes de production. Nous publions des mises à jour des fonctionnalités du portail et des applications environ toutes les 6 semaines, toujours corrigées pour inclure la version la plus récente des systèmes d'exploitation et des bibliothèques utilisés. Toute vulnérabilité critique est corrigée dès que possible dans une version de correctif conformément à notre politique de gestion des correctifs. Les informations sur la version actuelle du produit sont disponibles sur le site web de SHOEBOX : https://www.shoebox.md/software-updates/

Comme pour toutes les modifications en production, les tests (dans des environnements d'assurance qualité séparés) et la mise en production sont contrôlés via notre processus de conception et développement à étapes, qui est audité annuellement pour la conformité aux normes ISO 13485, IEC 62304 et ISO 27001.

Durcissement du système d'exploitation et des bases de données

Nous utilisons uniquement des images de système d'exploitation pré-durcies certifiées par Amazon pour construire notre plateforme. Par défaut, nos politiques de sécurité stipulent que tous les ports doivent être fermés, puis ouverts uniquement au minimum requis pour fournir l'accès à nos services.

Surveillance et journalisation du système

Amazon Cloudwatch surveille la santé de nos systèmes. Nous utilisons également un système flexible et évolutif pour centraliser les journaux d'accès, et nous surveillons ces journaux pour détecter toute activité suspecte. La journalisation couvre toutes les tentatives d'authentification, ainsi que toutes les demandes de création, de mise à jour, de suppression et de consultation des données des patients.

Réponse aux incidents, signalement des incidents et notification des violations

Nos politiques et procédures de réponse aux incidents, de communication et de signalement sont établies en conformité avec les normes ISO 27001 et ISO 13485. Nos systèmes de réponse aux incidents sont testés régulièrement.

Dans l'éventualité peu probable d'une violation, conformément à l'Addendum au traitement des données (DPA), nous nous engageons à notifier les clients concernés dans les 72 heures suivant la découverte.

En tant que sous-traitant des données, notre engagement principal en vertu du DPA est de vous soutenir et de vous assister, en tant que responsable du traitement, dans l'accomplissement de vos obligations au titre du RGPD, y compris les articles 33 et 34. En cas de violation de données personnelles, nous vous notifierons rapidement et sans retard injustifié, en fournissant toutes les informations pertinentes pour faciliter votre notification à l'autorité de contrôle comme l'exige l'article 33. Nous coopérerons également pleinement avec vous dans l'accomplissement de vos obligations au titre de l'article 34, en fournissant toute l'assistance et les informations nécessaires pour vous permettre de notifier les personnes concernées si une violation est susceptible d'entraîner un risque élevé pour leurs droits et libertés.

Continuité des activités

Chez SHOEBOX, des exercices formels de continuité des activités/reprise après sinistre (PCA/PRS) sur table ou des scénarios de simulation sont programmés trimestriellement.

SHOEBOX et Amazon ont défini des procédures de mode d'urgence et de reprise après sinistre conçues pour assurer la continuité des activités dans toute situation.

Sauvegardes des données

Notre système de sauvegarde fonctionne comme suit :

- Toutes les données du **SHOEBOX® Data Management Portal** sont sauvegardées quotidiennement.
- Les sauvegardes quotidiennes sont conservées pendant 1 an.
- Le journal de la base de données (modifications incrémentielles) est sauvegardé en temps réel.
- Les sauvegardes de la base de données sont stockées sur Amazon S3 et peuvent être récupérées en 6 heures.
- Les données dans le service de stockage S3 sont redondantes avec 3 copies de données dans différents emplacements physiques.

Notre stratégie de sauvegarde protège contre la corruption irréversible de la base de données.

Disponibilité et redondance du système

Notre solution met automatiquement à l'échelle les ressources en fonction de la charge et les répartit entre des centres de données physiquement séparés.

Temps d'arrêt planifié

Notre système a été conçu pour une disponibilité de 99,9 %. Cependant, lorsqu'un temps d'arrêt planifié est nécessaire, nous fournirons un préavis d'au moins 48 heures. Les temps d'arrêt planifiés (en plus de l'état du service en temps réel) sont publiés sur https://www.shoebox.md/status

Support technique

Le support téléphonique et par courriel est disponible de 9 h à 17 h, heure de l'Est (HE), via https://www.shoebox.md/support