DÉCLARATION DE SÉCURITÉ

Chez SHOEBOX Ltd. ("**SHOEBOX**"), la sécurité de vos données est essentielle. L'objectif de cette déclaration de sécurité est de fournir une vue d'ensemble de notre architecture de sécurité, de nos cadres de sécurité, de nos méthodes de traitement des données, de nos politiques, de nos procédures, de nos certifications et de notre conformité.

A propos des produits SHOEBOX

SHOEBOX® PureTest est un audiomètre basé sur un iPad qui est utilisé en conjonction avec le portail de gestion des données SHOEBOX pour effectuer des tests auditifs diagnostiques.

La plateforme SHOEBOX® est une plateforme audiologique en ligne (composée de **SHOEBOX® Remote** et de **SHOEBOX® Consult**) destinée à être utilisée pour effectuer des tests auditifs afin de diagnostiquer d'éventuels troubles otologiques.

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

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

SHOEBOX® Audiometry Standard et SHOEBOX® Audiometry Pro sont des dispositifs médicaux enregistrés dans certaines juridictions. Il s'agit d'audiomètres à base de tablettes qui effectuent des tests auditifs diagnostiques.

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

Collectivement, nous appelons ces produits les "**solutions SHOEBOX**".

Les produits fonctionnant sur iOS (iPad) sont **SHOEBOX® Audiometry Standard, SHOEBOX® Audiometry Pro et SHOEBOX® QuickTest** et sont collectivement appelés **SHOEBOX Apps.**

APERÇU DE LA SÉCURITÉ

Conformité juridique et réglementaire

SHOEBOX se conforme 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 GDPR, avec un accord sur le traitement des données (DPA) en place conformément à l'article 28 du GDPR.

SHOEBOX Ltd est certifié ISO 27001:2013 (depuis octobre 2021) par le British Standard Institute (BSI). Les solutions SHOEBOX sont hébergées sur Amazon AWS ou Heroku qui sont conformes à de multiples normes, y compris 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 propose également un BAA aux clients américains de son service SHOEBOX qui doivent se conformer à l'HIPAA. L'alignement sur les exigences de l'HIPAA concernant les garanties administratives 164.308, physiques 164.310 et techniques 164.312, les règles de confidentialité 164.5xx et la notification des violations (164.4xx) a fait l'objet d'un audit externe par ***HIPAA Solutions RX*** (qui a conclu que *"SHOEBOX avait réalisé l'une des analyses de risque de sécurité/de confidentialité HIPAA les plus **approfondies et les** plus **complètes** observées au fil des ans" et que le consultant "n'a pas pu identifier de risques importants/de vulnérabilités en matière de confidentialité qui n'auraient pas été pris en compte par SHOEBOX").* SHOEBOX met à jour chaque année et procède à un audit interne d'une feuille de travail HIPAA détaillée qui établit des références croisées entre nos contrôles et nos politiques et procédures qui font l'objet d'un audit selon la norme ISO 27001.

Évaluation et gestion des risques

SHOEBOX a obtenu la certification ISO 13485 pour son système de gestion de la qualité, qui comprend des exigences en matière de confidentialité et de sécurité qui se recoupent. L'analyse des risques est effectuée à la fois du point de vue du **dispositif médical** (préjudice pour le patient) et du point de vue de l'**actif informationnel** (vie privée du patient) en utilisant les cadres de gestion des risques des normes ISO 13485, ISO 27001, ISO 27005 et ISO 31000.

Gestion des fournisseurs

Nous utilisons un processus de gestion et d'évaluation des fournisseurs pour tous nos fournisseurs de logiciels, d'hébergement en nuage, de matériel, etc. Les fournisseurs doivent être approuvés par nos services réglementaires, financiers, juridiques et de sécurité. Tous les fournisseurs font l'objet d'un examen au moins une fois par an.

Collecte, transmission et stockage des données

Toutes les données saisies à l'aide des **applications SHOEBOX** sont stockées dans une base de données séparée qui est protégée par un "pare-feu" par rapport aux autres applications de l'iPad. Les sauvegardes sur des systèmes non conformes, tels qu'un ordinateur personnel, sont désactivées. Si elles sont sélectionnées, les données sont automatiquement sauvegardées sur AWS. Les données sont cryptées en transit (TLS v1.2 ou supérieur) et au repos (AES-256) une fois stockées dans le nuage.

Les **applications SHOEBOX** peuvent être utilisées pour collecter et transmettre certaines données au **service de stockage dans le nuage 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 de données

Le lieu d'hébergement des données dépend du pays du client :
- Pour les clients américains : Centre de données AWS en Virginie du Nord
- Pour les clients du reste du monde : Centre de données AWS du Canada central (Montréal)

Les données des clients et les sauvegardes de ces données ne sont jamais exportées hors du pays d'accueil.

Bien que SHOEBOX opère à partir d'un seul bureau situé à Ottawa, au Canada, aucune donnée client n'est jamais stockée sur le site.

Sécurité physique

L'entreprise a mis en place des politiques documentées qui interdisent le stockage d'informations de santé protégées (PHI) dans les bureaux de SHOEBOX ou sur les ordinateurs appartenant à SHOEBOX, les systèmes de messagerie, ou dans des services tiers autres que nos serveurs de production certifiés. Les données sont physiquement sécurisées dans les entrepôts de données d'Amazon uniquement. Ces installations sont surveillées et dotées de personnel 24×7 et les serveurs sont protégés dans des cages verrouillées. Les détails des dispositifs de sécurité étendus peuvent être trouvés sur la page de sécurité d'AWS.

Conservation des données

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

Contrôle d'accès

Par défaut, tous les produits SHOEBOX authentifient les utilisateurs par login/mot de passe. Le nom d'utilisateur doit être une adresse électronique. Avant de pouvoir utiliser le compte, l'utilisateur doit le vérifier en cliquant sur un lien qui lui est envoyé par courrier électronique.

Lorsque l'utilisateur définit initialement son mot de passe, nous le hachons avec PBKDF2 à l'aide d'un sel sécurisé généré de manière aléatoire et nous 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 originales en clair ne sont jamais conservées.

Les règles de complexité des mots de passe configurables comprennent : Longueur minimale, lettres et chiffres obligatoires, caractères supérieurs et inférieurs obligatoires, caractères spéciaux, tentatives de verrouillage, longueur de verrouillage, réutilisation du mot 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 Single Sign On (SSO) est disponible pour certains clients de SHOEBOX Portal (y compris l'administration de SHOEBOX Online) et de SHOEBOX Puretest s'ils ont un fournisseur d'identité existant (IdP), ET n'est disponible que si elle est explicitement proposée dans le cadre de votre onboarding.
(Note : SHOEBOX Standard, Pro, & QuickTest ne supportent pas le SSO).

SHOEBOX s'appuie sur Amazon Cognito pour permettre l'authentification unique (SSO) (introduit 2021-Q4) pour les utilisateurs de SHOEBOX Portal et SHOEBOX Puretest. Cela ajoute le support 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), permettant aux départements informatiques d'appliquer le MFA et de centraliser la gestion des comptes des utilisateurs de SHOEBOX.

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

Accès à l'environnement de production

Les solutions SHOEBOX sont conçues de manière à ce qu'aucun employé de SHOEBOX ne puisse accéder aux données des clients, sauf dans des circonstances exceptionnelles. Les développeurs de logiciels n'ont accès qu'à un environnement Staging séparé. Le déploiement des mises à jour de logiciels en production est effectué par une équipe de développement qui a un accès limité aux mises à jour de logiciels, mais qui 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 à mot de passe unique (OTP).

L'accès aux données des clients doit faire l'objet d'une demande spéciale de la part du client et être approuvé par la direction générale.

Sécurité des employés

Tous les employés ont fait l'objet d'une vérification de leurs antécédents criminels lorsque la loi l'autorise. Nous vérifions également les références, les qualifications et le casier judiciaire de tous nos examinateurs audiologiques.

Formation et sensibilisation

Tous les employés ayant accès aux PHI ont été formés aux exigences en matière de confidentialité des données (notamment HIPAA, PIPEDA et GDPR). Un programme automatisé de formation anti-phishing permet de vacciner les employés contre les campagnes d'ingénierie sociale.

Séparation du réseau de l'entreprise

Le réseau interne de SHOEBOX est entièrement séparé du réseau de production. Tous les ports des machines sont verrouillés par des groupes de sécurité à l'aide d'un pare-feu, ce qui ne laisse qu'un seul port disponible pour le réseau de gestion du trafic. L'ensemble du stockage utilise des volumes cryptés en permanence.

Assurance de la qualité et essais

SHOEBOX a mis en place un processus conforme à la norme ISO 13485 pour maintenir la qualité de ses logiciels. Toute modification du code est testée à l'aide d'une combinaison de tests de régression manuels et automatisés. Tous les changements de code sont testés dans des environnements QA et Staging distincts avant d'être diffusés.

Tests et vérifications de sécurité internes et externes

SHOEBOX effectue des tests de sécurité internes et externes pour vérifier l'intégrité de ses systèmes. Le code est automatiquement analysé au cours de notre processus de construction régulier. Nos employés sont formés aux meilleures pratiques de sécurité standard pour le développement de logiciels afin de minimiser le risque d'introduire des vulnérabilités dans notre code. Notre sélection de technologies encourage encore davantage ces pratiques. Par exemple, les attaques par injection SQL sont évitées grâce à l'utilisation exclusive d'instructions préparées pour l'accès aux bases de données. En outre, nous procédons régulièrement à des examens du code par des pairs. Les nouveaux problèmes sont suivis et attribués à notre équipe d'ingénieurs dans le cadre de notre processus d'examen quotidien.

L'entreprise fait appel à des testeurs de pénétration externes pour valider les contrôles de sécurité. Les tests portent sur la vulnérabilité de notre réseau et du code de nos applications.

Gestion des vulnérabilités et correctifs

Notre équipe d'ingénieurs surveille les alertes de sécurité provenant de sources multiples. Les alertes concernant les problèmes de sécurité et les correctifs pour l'infrastructure sont générées automatiquement. Les alertes de sécurité sont gérées et classées par ordre de priorité dans notre système de suivi des problèmes. Les problèmes validés sont ensuite assignés à notre

équipe d'ingénieurs pour y remédier. Tous les problèmes sont enregistrés, attribués et clôturés dans notre système de gestion des problèmes.

Notre équipe d'ingénieurs examine quotidiennement les dossiers en attente et les problèmes sont attribués en fonction des priorités. Les problèmes critiques sont surveillés quotidiennement et traités immédiatement s'ils ont des répercussions sur nos systèmes de production. Nous publions des mises à jour du portail et de l'application toutes les six semaines environ, qui sont toujours corrigées pour inclure la version la plus récente des systèmes d'exploitation et des bibliothèques utilisés. Toute vulnérabilité critique est corrigée dès qu'elle est disponible dans une version ponctuelle, 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 apportées à la production, les tests (dans des environnements d'assurance qualité distincts) et la diffusion sont contrôlés par notre processus de conception et de développement, qui fait l'objet d'un audit annuel de conformité aux normes ISO 13485, CEI 62034 et ISO 27001.

Durcissement du système d'exploitation et de la base de données

Nous n'utilisons que des images d'OS pré-durcies certifiées par Amazon pour construire notre plateforme. Par défaut, nos politiques de sécurité stipulent que tous les ports doivent être fermés et qu'ils ne doivent être ouverts qu'au minimum requis pour permettre l'accès à nos services.

Surveillance du système et journalisation

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 à la recherche d'activités suspectes. 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, déclaration d'incident et notification de brèche

Nos politiques et procédures de réponse aux incidents, de communication et d'établissement de rapports sont établies en conformité avec les normes ISO 27001 et ISO 13485. Nos systèmes de réponse aux incidents font l'objet d'exercices réguliers.

Dans le cas improbable d'une violation, conformément à l'addendum sur le traitement des données (DPA), nous nous engageons à informer les clients concernés dans les 72 heures suivant la découverte de la violation.

En tant que responsable du traitement des données, notre principal engagement au titre du RGPD est de vous soutenir et de vous aider, en tant que responsable du traitement des données, à remplir vos obligations au titre du GDPR, y compris les articles 33 et 34. En cas de

violation de données à caractère personnel, nous vous en informerons rapidement et sans retard injustifié, en vous 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 pour remplir vos obligations au titre de l'article 34, en vous 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

À SHOEBOX, des exercices formels de simulation ou des scénarios de BC/DR sont programmés tous les trimestres.

SHOEBOX et Amazon ont tous deux défini un mode d'urgence et des procédures de reprise après sinistre destinés à assurer la continuité des activités dans n'importe quelle situation.

Sauvegardes de données

Notre système de sauvegarde fonctionne comme suit :

- Toutes les données du **portail de gestion des données SHOEBOX®** sont sauvegardées quotidiennement.
- Les sauvegardes quotidiennes sont conservées pendant un an.
- Le journal de la base de données (modifications incrémentales des données) 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 du service de stockage S3 sont redondantes, avec trois copies des données dans des lieux physiques différents.

Notre stratégie de sauvegarde protège contre la corruption irréversible des bases de données.

Disponibilité et redondance des systèmes

Notre solution adapte automatiquement les ressources en fonction de la charge et les équilibre entre des centres de données physiquement séparés.

Temps d'arrêt programmé

Notre système a été conçu pour être disponible à 100 %. Toutefois, si un arrêt programmé est nécessaire, nous vous en informerons au moins 48 heures à l'avance. Les temps d'arrêt programmés (en plus de l'état du service en temps réel) sont affichés à l'adresse https://www.shoebox.md/status.

Support technique

Une assistance par téléphone et par courrier électronique est disponible de 8h00 à 20h00, heure normale de l'Est, à l'adresse https://www.shoebox.md/support.