Chez Biosency, nous prenons la sécurité et la confidentialité de vos données personnelles très au sérieux. Vous trouverez dans ce document une vue d'ensemble des mesures de sécurité, des informations utiles pour un usage sécurisé du dispositif médical Bora Care et des recommandations pour vous prémunir des risques de cybersécurité.

En cas d'incident de sécurité, de message d'alerte sur Bora Care ou si vous avez des questions en matière de sécurité, contactez le support de Biosency à support@biosency.com ou au 0800 910 073 (FR) / (+33)2 21 65 70 01.

Table des matières

BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860

DESCRIPTION DU DISPOSITIF

La solution « **Bora Care** » associe le dispositif connecté « **Bora Band** » à une plateforme web de télésurveillance « **Bora Connect** ». Les données cardio-respiratoires collectées par le dispositif « Bora Band » sont transmises à la plateforme « **Bora Connect** » par l'un des trois dispositifs de remonté de données détaillées ci-dessous. La solution « **Bora Care** » est destinée aux patients insuffisants respiratoires chroniques.

La solution « **Bora Care** » est composée :

- d'un dispositif connecté de mesure de paramètres cardio-respiratoires « **Bora Band** »,
- d'un dispositif assurant la transmission de données, qui peut être :
  - soit une borne de remontée de données « **NGDF**»
  - soit l'application « **Bora Connect for Home** » préinstallé sur un téléphone mobile en mode kiosque
  - soit l'application mobile « **Bora Connect** » installée sur le téléphone du patient
- d'une plateforme web « **Bora Connect** » permettant de surveiller à distance des patients insuffisants respiratoires.

La transmission de données est assurée via Bluetooth entre le dispositif « **Bora Band** » et le dispositif assurant la transmission des données. Ensuite les données sont transmises à la plateforme « **Bora Connect** » via le réseau mobile ou le Wi-Fi.

COMPÉTENCES REQUISES

Les clients doivent suivre une **formation dispensée par les équipes de Biosency, ou ses partenaires habilités,** pour pouvoir utiliser la solution.

L'installation, la configuration et l'utilisation de la solution ne demandent cependant **aucune compétence informatique** particulière.

SÉCURITÉ DU DISPOSITIF MÉDICAL

GOUVERNANCE ET ORGANISATION DE LA SECURITE

Biosency a établi une **structure** et un **système de gouvernance** en matière de sécurité conformes aux normes applicables. Cette structure comprend des référents de la sécurité et des experts techniques qui participent activement aux opérations quotidiennes de sécurité.

SÉCURITÉ DES RESSOURCES HUMAINES

Les contrats des employés de Biosency comprennent une **clause de confidentialité** qui couvre les informations auxquelles ils ont accès dans le cadre de leurs activités et responsabilités, ainsi que les **risques encourus en cas de non-respect** de ces obligations. Une **charte informatique** énonce également leurs obligations en matière de protection des données.

En conformité avec la législation en vigueur, des **vérifications sont réalisées pour tous les nouveaux employés**. Le personnel R&D et administratif est soumis à des vérifications spécifiques avant d'obtenir l'accès aux systèmes et aux zones restreintes.

Enfin, Biosency maintient un **programme permanent de sensibilisation aux principes du Règlement Général de Protection des Données (RGPD)**, à la sécurité et la confidentialité des données pour tous ses employés.

BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860

CHIFFREMENT DES DONNÉES ET HÉBERGEMENT

« Bora Care » assure la confidentialité et l'intégrité des données en transit et au repos grâce au chiffrement des données et selon les bonnes pratiques en la matière.

L'hébergement de ces données est assuré par **une société partenaire Claranet**, certifiée Hébergeur de Données de Santé (HDS) et ISO 27001.

GESTION DES INCIDENTS ET INFORMATION

A Biosency, des procédures internes régissent la gestion des réclamations client et la gestion des incidents de matériovigilance, de sécurité ou de violation de données. Ces procédures internes garantissent une gestion efficace des réclamations et des incidents, assurant ainsi la sécurité, la conformité réglementaire, et la satisfaction des utilisateurs. Ces procédures se reposent également sur les procédures de gestion des incidents et de gestion de crise de Claranet, qui sont décrites dans le **Plan d'Assurance Qualité**.

A Biosency, des procédures internes régissent la communication externe. Ces procédures garantissent une communication claire et rapide avec les clients et toute autre partie prenante. La communication de Claranet vers Biosency se fait par l'envoi d'un avis d'incident par mail.

CONTRAT DE SERVICE LEVEL AGREEMENT (SLA)

Nous offrons une disponibilité continue de 24 heures sur 24 et 7 jours sur 7. Biosency s'efforcera de remettre en état de fonctionnement la plateforme Bora connect® dans les meilleurs délais. À défaut de résolution de l'incident au plus tard dans les cinq jours ouvrés à compter de la réception de l'appel par un utilisateur, Biosency devra mettre en œuvre une solution de remplacement de nature pour lui permettre d'assurer les fonctions vitales de la plateforme Bora connect®, cela pendant la durée nécessaire à la résolution de l'incident.

EXIGENCES ET RECOMMANDATIONS MINIMALES DE SÉCURITÉ

Sur le principe de séparation des usages informatiques, il est fortement recommandé d'utiliser uniquement un **poste de travail professionnel** pour accéder à la plateforme web.

Il est conseillé d'utiliser un ordinateur équipé d'un logiciel **antivirus** et d'un **pare-feu** pour prévenir l'accès de trafic non autorisé au réseau sécurisé.

Les outils numériques (système d'exploitation, navigateur web, logiciels, …) doivent être **mis à jour** régulièrement.

Enfin, il est recommandé d'utiliser un **réseau internet de confiance** configuré avec des mesures de sécurité appropriées pour garantir une utilisation sécurisée de la plateforme web.

Toutes ces recommandations sont développées dans les chapitres suivants.

MISES À JOUR DE SÉCURITÉ

Il est important de ne pas empêcher les mises à jour automatiques des dispositifs de la solution Bora care.

DISPOSITIF BORA CARE

Le déploiement des mises à jour de sécurité des composants de la solution « Bora Care » sont effectués de la façon suivante :

- Pour le dispositif connecté **« Bora band »** : la connexion régulière au téléphone ou à la borne de remontée des données assurera une mise à jour automatique du dispositif.

BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860

- Pour l'application mobile **« Bora connect »** : Vous pouvez obtenir les mises à jour sur la boutique d'applications de votre smartphone, que ce soit le Play Store ou l'App Store. Nous recommandons cette mise à jour dès que lors qu'une nouvelle version est disponible. Le cas échéant, vous êtes notifié au lancement de l'application.
- Pour la borne de remontée de données « **NGDF**» : la mise à jour du logiciel embarqué se fera au moyen d'un renvoi à Biosency ou tout autre prestataire habilité.
- Pour l'application « **Bora Connect for Home** » préinstallé sur un téléphone mobile en mode kiosque : les mises à jour sont déployées automatiquement par Biosency.
- Pour la Plateforme web « **Bora Connect** » : les mises à jour sont déployées automatiquement par Biosency.

SYSTÈME D'EXPLOITATION DU TÉLÉPHONE

Avant d'utiliser la solution « Bora Care » et afin de garantir que vous bénéficiez des dernières mises à jour de sécurité pour votre téléphone, assurez-vous que votre téléphone dispose de la **dernière version du système d'exploitation** (OS).

ENVIRONNEMENT D'UTILISATION PRÉVU

Le dispositif Bora Care est prévu pour être utilisé dans les environnements suivants :

- **Domicile du patient**
- **Structure de santé**
- **Cabinet médical**.

L'accès à la plateforme web nécessite l'utilisation d'un **ordinateur dont la sécurité est gérée par l'organisation utilisatrice**. L'utilisation de la plateforme web à partir **d'un ordinateur ou d'un téléphone non sécurisé comprend un risque de compromission des comptes** des professionnels de santé, des acteurs de santé ou des patients. Cela peut également exposer l'utilisateur à une perte de confidentialité, à des menaces de vol d'identité et créer d'autres vulnérabilités en matière de cybersécurité.

CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES

Le dispositif médical « Bora Care » distingue 4 rôles dont les accès, droits et privilèges sont spécifiques et différents :

- **Administrateur** : peut créer et gérer les comptes des acteurs de santé et des professionnels de santé.
- **Professionnel de santé :** peut consulter les données de santé des patients qu'il suit.
- **Acteur de santé** : permet à l'utilisateur de gérer les comptes des acteurs de santé, des patients et de gérer la flotte de dispositifs sous sa responsabilité. L'acteur de santé peut également accéder aux données de santé des patients de sa structure.
- **Patient :** peut consulter ses propres données de santé et modifier ses informations personnelles.
- **Biosency** : peut créer les structures d'acteur de santé, les comptes professionnels de santé et les comptes administrateur. Cet utilisateur ne peut pas accéder aux données de santé des patients.

BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860

AUTHENTIFICATION ET MOT DE PASSE

Les mots de passe utilisés pour se connecter à la plateforme web Bora connect doivent respecter les normes de mot de passe définies par Biosency dans le manuel utilisateur de Bora connect, disponible sur doc.bora-connect.com.

Il est recommandé d'utiliser des mots de passe **longs**, **complexes**, **sans informations personnelles**, **uniques** et **secrets**.

La **double authentification** est activée pour tous les comptes.

Le compte des utilisateurs est bloqué après plusieurs **tentatives de connexion consécutives infructueuses.**

UTILISATION DES RÉSEAUX

Ne faites pas confiance aux réseaux non maitrisés pour connecter vos équipements et consulter des données sensibles comme des données de santé.

RÉSEAUX PUBLICS ET PRIVÉS

L'utilisation de **réseaux publics** peut représenter une **menace** pour la confidentialité de vos données, car des **tiers malveillants** pourraient essayer d'y accéder. Par conséquent, il est fortement conseillé d'utiliser une **connexion Internet privée** et **maitrisée** pour **protéger vos informations sensibles.**

WI-FI

Afin de garantir la sécurité et la confidentialité de vos données lors de l'utilisation de la plateforme Bora Connect, il est recommandé d'utiliser une connexion **Wi-Fi sécurisée** par un protocole de type **WPA2 minimum.**

SURVEILLANCE, VOL ET DÉGRADATION

Ne laissez pas le dispositif Bora band sans surveillance sous peine de le voir manipulé, compromis à votre insu et vos données volées.

Le dispositif Bora Band est conçu de tel sorte qu'un haut niveau de sécurité des données soit assuré. Cependant les clients et utilisateurs veilleront à surveiller et assurer l'intégrité du dispositif.

IDENTIFIANTS PLATEFORME

Assurez-vous de **protéger soigneusement vos informations de connexion**, y compris votre identifiant et votre mot de passe.

De plus, **sécurisez l'accès à votre smartphone** avec un code PIN ou une reconnaissance biométrique pour empêcher un accès non autorisé à vos données.

Vos informations de connexion sont **strictement personnelles** et ne doivent pas être partagées avec des tiers.

AVERTISSEMENTS

RISQUES INFORMATIQUES LIÉS AU DISPOSITIF

Le dispositif Bora Band peut être exposé à d'éventuelles attaques qui pourraient perturber son bon fonctionnement. Par exemple, il est possible que des attaques visant à saturer le canal de communication Bluetooth soit menées de manière à perturber ou interrompre la

BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860

connectivité. Cependant, **il est important de noter que cela n'affecte pas la sécurité de vos données**, mais peut entraîner des problèmes de transmission avec le reste du dispositif.

En cas de suspicion, n'hésitez pas à contacter immédiatement votre prestataire de services.

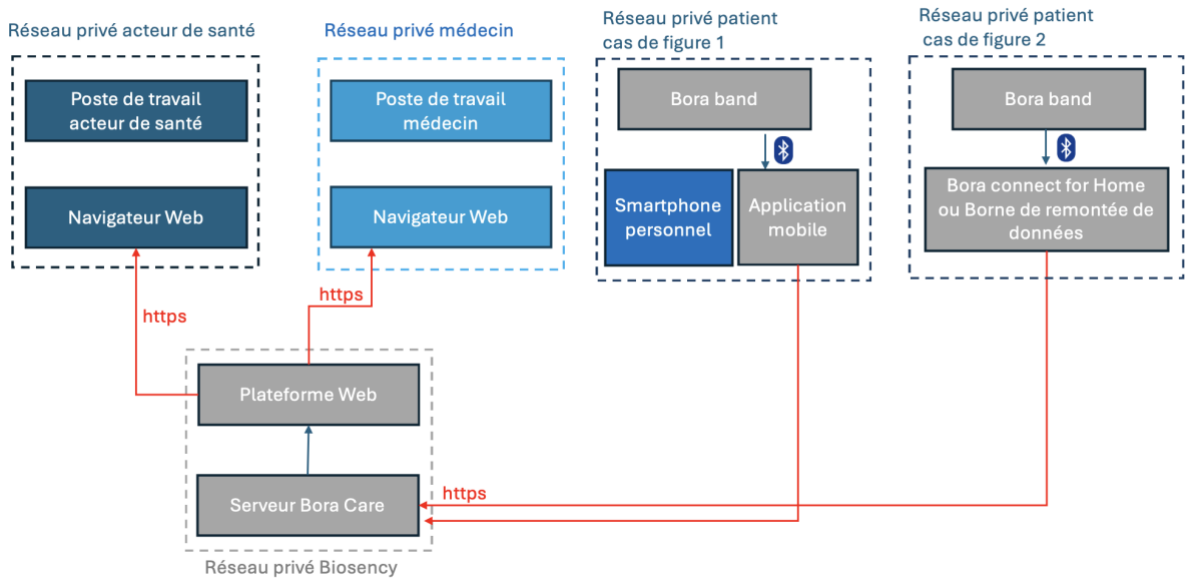
RISQUES INFORMATIQUES LIÉS AU MODULE BORA PARTNER

Des données sensibles sont transmises par l'intermédiaire de l'API REST « Bora Partner ». Il est vivement recommandé à tous les partenaires de mettre en place des mesures de sécurité appropriées. Cela inclut : **la restriction et la gestion des droits d'accès, l'utilisation et l'historisation de journaux d'activité (logs), la détection d'intrusion, l'usage d'antivirus et antimalwares, ...**

INFORMATIONS DE SÉCURITÉ

Biosency fournit sur demande un tableau décrivant l'ensemble des mesures de sécurité intégrées dans le dispositif « Bora Care ». Ce tableau utilise le format MDS2 (Manufacturer Disclosure Statement for Medical Device Security), qui est un standard répandu dans le domaine des dispositifs médicaux.

CARTOGRAPHIE DU DISPOSITIF BORA CARE



BIOSENCY, 13 rue Claude Chappe, 35510 Cesson-Sévigné. Société par Actions Simplifiées immatriculée sous le SIREN 830861860
N° TVA intracommunautaire FR66830861860