**At Biosency, we take the security and confidentiality of your personal data very seriously. In this document, you'll find an overview of security measures, useful information for the safe use of the Bora Care medical device, and recommendations for protecting yourself against cybersecurity risks.**

**In the event of a security incident or alert message on Bora Care, or if you have any security questions, please contact Biosency support at support@biosency.com or 0800 910 073 (FR) / (+33)2 21 65 70 01.**

# Table of contents






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

N° TVA intracommunautaire FR66830861860

# DEVICE DESCRIPTION

The "**Bora Care**" solution combines the "**Bora Band**" connected device with the "**Bora Connect"** web-based remote monitoring platform. Cardio-respiratory data collected by the "Bora Band" device are transmitted to the "**Bora Connect**" platform via one of the three data transmission devices detailed below. The "**Bora Care**" solution is designed for patients with chronic respiratory insufficiency.

The "**Bora Care**" solution consists of:

- a "**Bora Band**" connected device for measuring cardio-respiratory parameters,
- a data transmission device, which may be:
  - the data upload terminal "**NGDF**"
  - or the "**Bora Connect for Home**" application preinstalled on a cell phone in kiosk mode
  - or the "**Bora Connect**" mobile application installed on the patient's phone
- the "**Bora Connect**" web platform for remote monitoring of patients with respiratory insufficiency.

Data transmission takes place via Bluetooth between the "**Bora Band**" device and the device transmitting the data. The data is then transmitted to the "**Bora Connect**" platform via the mobile network or Wi-Fi.

# SKILLS REQUIRED

Customers are required to undergo training by Biosency teams, or authorized Biosency partners, in order to use the solution.

Installation, configuration and use of the solution require no special **IT skills**.

# MEDICAL DEVICE SAFETY

## SECURITY GOVERNANCE AND ORGANIZATION

Biosency has established a security **governance structure** and **system in** line with applicable standards. This structure includes security referents and technical experts who are actively involved in day-to-day security operations.

## HUMAN RESOURCES SECURITY

Biosency employees' contracts include a **confidentiality clause** covering the information to which they have access in the course of their activities and responsibilities, as well as the **risks incurred in the event of non-compliance** with these obligations. An **IT charter** also sets out their obligations in terms of data protection.

In compliance with current legislation, **checks are carried out on all new employees**. R&D and administrative staff undergo specific checks before being granted access to systems and restricted areas.

Finally, Biosency maintains an ongoing program to raise awareness of the principles of the General Data Protection Regulation (GDPR), data security and confidentiality for all its employees.



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

N° TVA intracommunautaire FR66830861860

## DATA ENCRYPTION AND HOSTING

"Bora Care ensures the confidentiality and integrity of data in transit and at rest, thanks to data encryption in line with best practices.

Data is hosted by **Claranet**, **a partner company** certified as a Health Data Host (HDS) and ISO 27001.

## INCIDENT MANAGEMENT AND INFORMATION

At Biosency, internal procedures govern the handling of customer complaints and the management of material safety, security or data breach incidents. These internal procedures guarantee effective claims and incident management, ensuring safety, regulatory compliance and user satisfaction. These procedures are also based on Claranet's incident and crisis management procedures, which are described in the **Quality Assurance Plan**.

At Biosency, internal procedures govern external communication. These procedures guarantee clear and rapid communication with customers and other stakeholders. Claranet communicates with Biosency by sending a notice of incident by e-mail.

## SERVICE LEVEL AGREEMENT (SLA)

We offer continuous availability 24 hours a day, 7 days a week. Biosency will endeavor to restore the Bora connect® platform to working order as quickly as possible. If the incident is not resolved at the latest within five working days of receipt of the call by a user, Biosency shall implement a replacement solution of a nature to enable it to ensure the vital functions of the Bora connect® platform, for the time necessary to resolve the incident.

## MINIMUM SAFETY REQUIREMENTS AND RECOMMENDATIONS

On the principle of separation of IT uses, it is strongly recommended to use only a **professional workstation** to access the web platform.

We recommend using a computer equipped with **antivirus** software and a **firewall** to prevent unauthorized traffic accessing the secure network.

Digital tools (operating system, web browser, software, etc.) must be updated regularly. Finally, we recommend using a **trusted Internet network** configured with appropriate security measures to guarantee secure use of the web platform.

All these recommendations are developed in the following chapters.

## SECURITY UPDATES

It is important not to prevent automatic updates of Bora care solution devices.

### BORA CARE

Security updates for components of the "Bora Care" solution are deployed as follows:

- For the **"Bora band**" connected device: regular connection to the telephone or to the data feedback terminal will ensure that the device is automatically updated.
- For the **"Bora connect"** mobile application: You can obtain updates from your smartphone's application store, either the Play Store or the App Store. We recommend that you update as soon as a new version is available. You'll be notified when the application is launched.
- For the "**NGDF**" data feedback terminal: the embedded software will be updated by



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

N° TVA intracommunautaire FR66830861860

sending back the terminal to Biosency or any other authorized service provider.

- For the "**Bora Connect for Home**" application preinstalled on a cell phone in kiosk mode: updates are deployed automatically by Biosency.
- For the "**Bora Connect**" web platform: updates are deployed automatically by Biosency.

### PHONE OPERATING SYSTEM

Before using the "Bora Care" solution and to ensure that you benefit from the latest security updates for your phone, please make sure that your phone has the **latest version of the operating system** (OS).

## INTENDED ENVIRONMENT OF USE

The Bora Care device is designed for use in the following environments:

- **Patient's home**
- **Health structure**
- **Medical practice**.

Access to the web platform requires the use of a computer whose security is managed by the user organization. Using the web platform from an unsecured computer or phone involves the risk of compromising the accounts of healthcare professionals, healthcare actors or patients. It can also expose the user to loss of confidentiality, threats of identity theft and create other cybersecurity vulnerabilities.

## ROLE-BASED ACCESS CONTROL

The "Bora Care" medical device distinguishes 4 roles with specific and different accesses, rights and privileges:

- **Administrator**: can create and manage accounts for healthcare professionals.
- **Healthcare professionals:** can consult the health data of patients under their care.
- **Healthcare actor**: enables the user to manage the accounts of healthcare actors and patients, and to manage the fleet of devices under his responsibility. The healthcare actor can also access the health data of patients within his structure.
- **Patient:** can consult his or her own health data and modify personal information.
- **Biosency**: can create healthcare actor structures, healthcare professional accounts and administrator accounts. This user cannot access patient health data.

## AUTHENTICATION AND PASSWORD

Passwords used to connect to the Bora connect web platform must comply with the password standards defined by Biosency in the Bora connect user manual, available at doc.bora-connect.com.

We recommend using long, complex, unique and secret passwords that contain no personal information.

**Two-factor authentication** is enabled for all accounts.

User accounts are blocked after several consecutive unsuccessful login attempts.



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

N° TVA intracommunautaire FR66830861860

### NETWORK UTILIZATION

Don't trust uncontrolled networks to connect your equipment and consult sensitive data such as health data.

#### PUBLIC AND PRIVATE NETWORKS

Using **public networks** can pose a **threat to** the confidentiality of your data, as **malicious third parties** may try to gain access. Therefore, we strongly advise you to use a **private** and **controlled Internet connection** to **protect your sensitive information.**

#### WI-FI

To guarantee the security and confidentiality of your data when using the Bora Connect platform, we recommend using a **Wi-Fi** connection **secured** by a **WPA2** protocol **or higher.**

### SURVEILLANCE, THEFT AND DAMAGE

**Don't leave your Bora band device unattended**, otherwise it could be manipulated, compromised without your knowledge, and your data stolen.

The Bora Band device is designed to ensure a high level of data security. However, customers and users are responsible for monitoring and ensuring the integrity of the device.

### PLATFORM LOGIN

Be sure to **protect your login details**, including your username and password.

In addition**, secure access to your smartphone** with a PIN code or biometric recognition to prevent unauthorized access to your data.

Your login information is **strictly personal** and must not be shared with third parties.

## WARNINGS

### IT RISKS RELATED TO THE SYSTEM

The Bora Band device may be exposed to attacks that could disrupt its operation. For example, it is possible that attacks aimed at saturating the Bluetooth communication channel could be carried out in such a way as to disrupt or interrupt connectivity. However, **it is important to note that this does not affect the security of your data**, but may lead to transmission problems with the rest of the device.

In case of suspicion, don't hesitate to contact your service provider immediately.

### IT RISKS ASSOCIATED WITH THE BORA PARTNER MODULE

Sensitive data is transmitted via the "Bora Partner" REST API. All partners are strongly advised to implement appropriate security measures. These include **restriction and management of access rights, use and archiving of activity logs, intrusion detection, use of anti-virus and anti- malware software, etc.**

## SAFETY INFORMATION

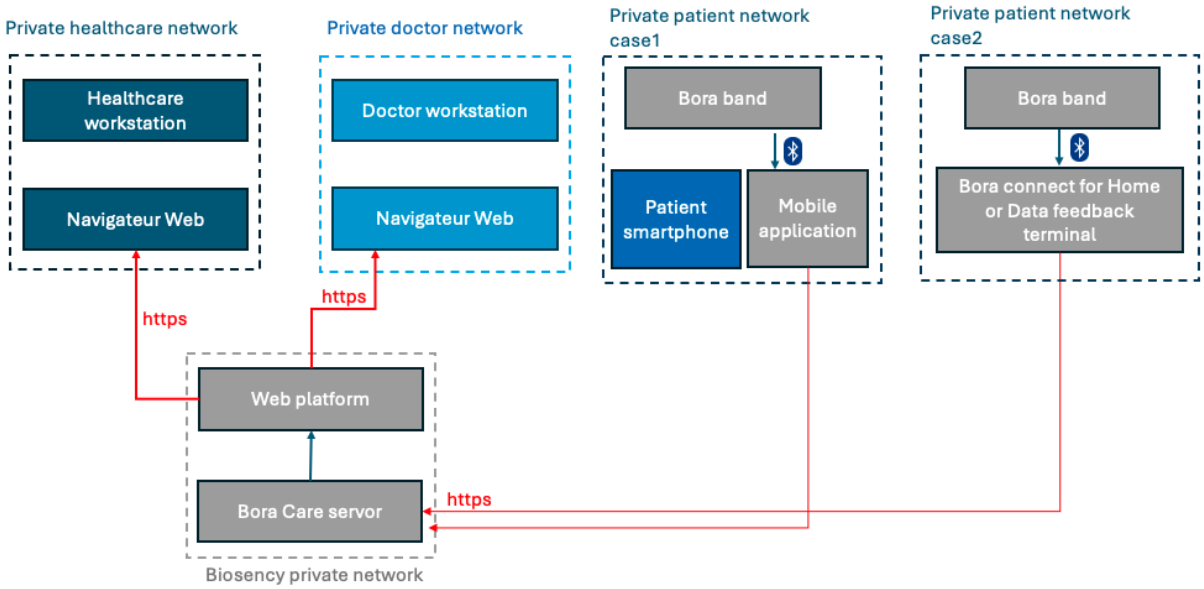
On request, Biosency can supply a table describing all the safety measures integrated into the "Bora Care" device. This table uses the MDS2 (Manufacturer Disclosure Statement for Medical Device Security) format, a widespread standard in the medical device industry.



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

N° TVA intracommunautaire FR66830861860

## MAPPING THE BORA CARE SYSTEM






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

N° TVA intracommunautaire FR66830861860