PERSONAL DATA PROTECTION POLICY –

BORA CARE® PREAMBLE

Who is this policy aimed at?

This data protection policy is intended for Users of the Bora care® solution, i.e.:
- **Patients;**

- **employees of BIOSENCY customers**, i.e. healthcare establishments, home healthcare providers, nursing homes, etc.;

- **and Healthcare Professionals who consult Patient data** as part of their remote monitoring by BIOSENCY Customers,

in order to inform them in detail of the personal data processing that concerns them and that BIOSENCY implements.

Within the framework of the use of the Bora care® Solution, personal data concerning the User will be collected and processed by BIOSENCY.

BIOSENCY is committed to ensuring that the processing it implements complies with legislation relating to the protection of personal data, including the provisions of European Regulation (EU) 2016/679 of 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("GDPR"), as well as French Law n°78-17 relating to data processing, files and freedoms as amended (French Data Protection Act).

This data protection policy does not cover the processing of personal data implemented by BIOSENCY's Customers (healthcare establishments, home healthcare service providers, nursing homes, etc.) and Healthcare Professionals, for which they are the data processors. Users are invited to contact BIOSENCY's Customers (healthcare establishments, home healthcare service providers, nursing homes, etc.) and Healthcare Professionals to obtain information on this processing.

Definitions:

For the purposes of this personal data protection policy, the definitions of "personal data" and "data controller" are those set out in Article 4 of the GDPR.

What is the purpose of this policy?

Biosency, which manages the Bora care® solution and in particular the Bora connect® platform, attaches great importance to the protection and confidentiality of your personal data, which for us represents a guarantee of reliability and trust.

The Data Privacy Policy specifically reflects our **commitment to ensuring that Biosency complies with applicable data protection rules** and, in particular, those of the General Data Protection Regulation ("GDPR").

In particular, the privacy policy aims to inform you about how and why we process your data in connection with the **services** we provide.

Who does this policy apply to?

The policy applies to all users of our Bora care® solution, regardless of where they live.

Why do we process your data?

Part intended for Patients

As part of the services we offer, we must process your personal data:

- **So that you can use and benefit from our service and all its functions** on the basis of our general conditions of use.
- **To manage user accounts** (e.g. account creation, access to the service and account deletion) on the basis of our general conditions of use.
- **So that you can receive our technical emails and SMS messages (e.g. password changes, notifications, alerts, etc.)** which are essential for the proper operation of our service on the basis of our general conditions of use.
- **So that we can analyse your health data for research purposes,** on the basis of your prior consent.

- **To guarantee and improve the security and quality of our** day-to-day **services** (e.g. statistics, data security, etc.) on the basis of our legal obligations, our general conditions of use and our legitimate interest in ensuring the proper functioning of our services.

- For patients as part of remote medical monitoring - **To manage the transmission of invoices** relating to our services to social security and any complementary organisations on the basis of your consent and our contractual commitment.

Your data is collected **directly from you** when you use our service and we undertake to process your data only for the **purposes described above**.

Section for Employee(s)

As part of the services we offer, we must process your personal data:

- **So that you can use and benefit from our service and all its functions** on the basis of our general conditions of use.

- **To manage user accounts** (e.g. account creation, access to the service and account deletion) on the basis of our general conditions of use.

- **So that you can write your own comments on the management of your files** on the basis of our general conditions of use.

- **So that you can receive our technical emails and SMS messages (e.g. password changes, notifications, alerts, etc.)** which are essential for the proper operation of our service on the basis of our general conditions of use.

- **So that you can download and import documents onto our platform** on the basis of our general conditions of use.

- **To guarantee and improve the security and quality of our** day-to-day **services** (e.g. statistics, data security, etc.) on the basis of our legal obligations, our general conditions of use and our legitimate interest in ensuring the proper functioning of our services.

- **To keep you informed of our latest news** on the basis of our legitimate interest.

- **So that you can follow the training courses delivered on the platform** on the basis of our general conditions of use.

- **To manage the contractual relationship with Biosency's customers (invoicing, dispute management)** on the basis of our legitimate interest.

Your data is collected **directly from you** when you use our service and we undertake to process your data only for the **purposes described above**.

Part intended for healthcare professionals

As part of the services we offer, we must process your personal data:

- **So that you can use and benefit from our service and all its functions** on the basis of our general conditions of use.

- **To manage user accounts** (e.g. account creation, access to the service and account deletion) on the basis of our general conditions of use.

- **So that you can write your own comments on the management of your files** on the basis of our general conditions of use.

- **So that you can receive our technical emails and SMS messages (e.g. password changes, notifications, alerts, etc.)** which are essential for the proper operation of our service on the basis of our general conditions of use.

- **To guarantee and improve the security and quality of our** day-to-day **services** (e.g. statistics, data security, etc.) on the basis of our legal obligations, our general conditions of use and our legitimate interest in ensuring the proper functioning of our services.

Your data is collected **directly from you** when you use our service and we undertake to process your data only for the **purposes described above**.

Part intended for Distributors

As part of our contractual relationship, we must process your personal data:

- **To perform our contract** on the basis of our contractual commitment and on the basis of our legitimate interest.
- **To manage our invoicing and accounting** on the basis of our legal obligations.
- **So that you can use and benefit from our service and all its functions** on the basis of our general conditions of use.
- **To manage user accounts** (e.g. account creation, access to the service and account deletion) on the basis of our general conditions of use.
- **So that you can receive our technical emails and SMS messages (e.g. password changes, notifications, alerts, etc.)** which are essential for the proper operation of our service on the basis of our general conditions of use.
- **To guarantee and improve the security and quality of our** day-to-day **services** (e.g. statistics, data security, etc.) on the basis of our legal obligations, our general conditions of use and our legitimate interest in ensuring the proper functioning of our services.

Your data is collected **directly from you**.

However, when you voluntarily publish content on the pages that we publish on social networks, you acknowledge that you are **entirely responsible for** any personal information that you may transmit, whatever the nature and origin of the information provided.

What data do we process and for how long?

We have summarised the **categories of personal data** we collect and their **respective retention periods**.

If you would like further details on the retention **periods** applicable to your data, please contact us at dpo@biosency.com.

Part intended for Patients, Employees and Healthcare Professionals

- **Personal identification data** (e.g. surname, first name) and **contact details** (e.g. email address, telephone number, etc.) are kept for the duration of the service, plus the statutory limitation periods, which are generally 5 years.

- **Email address and telephone number to receive our technical messages by email and SMS**. These details will be kept until your account is deleted.

- **Connection data** (e.g. logs, IP address, etc.) kept for 1 year.

- For Patients only - **Health data** retained until your account is deleted.

- For Patients only - **Specific data** (social security number, data relating to your supplementary health insurance) kept for the period during which your account is activated, plus the period for which invoices are kept (10 years).

Once the retention periods described above have expired, the deletion of your personal data is **irreversible** and we will no longer be able to communicate it to you after this period. At most, we may only keep anonymous data for **statistical** purposes.

Please also note that in the event of a **dispute**, we are obliged to retain **all** data concerning you for the duration of the case, even after the expiry of the retention periods described above.

Part intended for Distributors

- **Professional identification data** (e.g. surname, first name, position, company, etc.) and **contact details** (e.g. e-mail address and business telephone number, etc.) kept for the duration of our contractual relationship, plus the statutory limitation periods, which are generally 5 years.

- **When there is confusion between the name of your organisation and your personal name (e.g. self-employed entrepreneur, very small business, etc.), or between economic and financial data (e.g. bank account number, verification code, etc.)**, these are kept for the time required for the transaction and for managing invoicing and payments, plus the statutory limitation periods, which are generally 5 to 10 years.

- Your **email address** will be kept for a maximum of 3 years from the date of your last contact with us, for the purposes of **our email marketing campaigns**.

- **Telephone number for our commercial telephone prospecting campaigns**, kept for a maximum of 3 years from the last contact we had with you.

- **Email address to receive our newsletter**, retained until the end of your newsletter subscription.

Once the retention periods described above have expired, the deletion of your personal data is **irreversible** and we will no longer be able to communicate it to you after this period. At most, we may only keep anonymous data for **statistical** purposes.

Please also note that in the event of a **dispute**, we are obliged to keep **all** your personal data for as long as the case is being processed, even after the retention periods have expired

What rights do you have to control the use of your data?

The applicable data protection regulations give you **specific rights** which you can exercise, **at any time** and **free of charge**, to control the use we make of your data.

- The right to **access** and **copy** your personal data, provided that this request does not conflict with business secrecy, confidentiality or the confidentiality of correspondence.

- The right to **rectify** any personal data that is incorrect, obsolete or incomplete.

- The right to request the **deletion** ("right to be forgotten") of your personal data that is not essential for the proper functioning of our services.

- The right to **limit** your personal data, which allows you to take a snapshot of the use of your data in the event of a dispute over the legitimacy of processing.

- The right to data **portability**, which allows you to recover part of your personal data so that it can be easily stored or transmitted from one information system to another.

- The right to give **instructions** on what should happen to your data in the event of your death, either through you, a trusted third party or a beneficiary.

For a request to be **implemented**, it must be sent directly by **you** to dpo@biosency.com. Any request that is not made in this way **cannot be processed**.

Requests cannot come from anyone other than you. We may therefore ask you to provide **proof of identity** if there is any doubt about the applicant's identity.

We will respond to your request as quickly as **possible**, within **one month** of receipt, unless the request is complex or repeated. In this case, the **maximum** response time is **three months**.

Please note that we can always **refuse** to respond to any **excessive or unfounded** request, particularly if it is **repetitive**.

Who can access your data?

WE NEVER TRANSFER OR SELL YOUR DATA TO THIRD PARTIES OR COMMERCIAL PARTNERS. ALL YOUR PERSONAL DATA IS USED EXCLUSIVELY BY OUR TEAMS OR BY OUR IT SERVICE PROVIDERS.

More specifically, we only share your data with people who are **duly authorised** to use it to provide you with our service, such as our IT department, our customer relations department, as well as the healthcare professionals and employees of Biosency's customers (e.g. the medical staff of Biosency's hospitals): home health care providers, nursing homes, etc.), who are authorised to access patients' health data.

Your personal data is also transferred to our IT service providers who are used solely to operate our service, such as our data host or our technical email sending tool.

We would like to point out that we **check all our IT service providers before recruiting them** to ensure that they scrupulously comply with the applicable data protection rules.

How do we protect your data?

We use all the **technical** and **organisational means required** to guarantee the **security** of your data on a day-to-day basis and, in particular, to combat any risk of unauthorised destruction, loss, alteration or disclosure of your data (e.g. training, access control, passwords, etc.).

Can your data be transferred outside the European Union?

Unless strictly necessary and on an exceptional basis, we never transfer your data outside the European Union and your data is always hosted on **European soil**. In addition, we do our utmost to only recruit service providers who host your data within the European Union.

Where we use service providers located outside the European Union, we take great care to ensure that they always implement **appropriate guarantees to ensure the confidentiality and protection of your data**. In addition, we undertake to always enter into Standard Contractual Clauses with them, drawn up by the European Commission, in order to provide a framework for such transfers.

Who can you contact for more information?

You can contact our DPO free of charge at any time at dpo@biosency.com to obtain more information or details on how we process your data.

To guarantee the protection and integrity of your data, we have officially appointed an **independent Data Protection Officer** ("**DPO**") at our supervisory authority.

How can you contact the French data protection authority (CNIL)?

You may contact the **"French data protection authority"** or **"CNIL"** at any time at the following address: CNIL Complaints Department, 3 place de Fontenoy – TSA 80751, 75334 Paris Cedex 07 or by telephone on 01.53.73.22.22.

Can the policy be changed?

We may amend our privacy policy at **any time** to adapt it to new **legal requirements** and to **new processing operations** that we may carry out in the future.