

Advanced Brain Monitoring, Inc. (ABM) is a neuro-diagnostics device company internationally recognized for its innovative technologies. Our products are used by individuals, clinicians, researchers, and in clinical trials to interpret brain and physiological function as they relate to chronic diseases and early stage neurodegeneration, as well as to improve sleep quality and enhance performance. ABM is an ISO 13485 and FDA device manufacturer. We have a global distribution network established in the EU, Asia, and Australia. ABM is based in Carlsbad, CA with a European office in Belgrade, Serbia.

PRIVACY COMMITMENT STATEMENT

ABM is committed to protecting your privacy and developing technology that gives you the most powerful and safe online experience. Consistent with this commitment, ABM maintains compliance with several regulatory programs. We are dedicated to ensuring compliance with all of our products and services, as well as the underlying processing of personal data on behalf of our customers.

- Health Insurance Portability and Availability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
- The European Union (EU) General Data Protection Regulation (GDPR)
- EU-US and Swiss-US Privacy Shield Frameworks (Privacy Shield)

ABM is HIPAA compliant. HIPAA establishes standards for the security of electronic protected health information. We perform periodic technical and non-technical evaluations that establish the extent to which our security policies and procedures meet the HIPAA security requirements. The U.S. Department of Health and Human Services (HHS) does not currently offer HIPAA certification. Please visit the HHS website to [learn more about HIPAA](#).

ABM is HITECH compliant. HITECH promotes the adoption and meaningful use of health information technology, as well as privacy and security concerns associated with the electronic transmission of health information. HHS does not currently offer HITECH certification. Please visit the HHS website to [learn more about HITECH](#).

ABM maintains Privacy Shield certifications for the EU-US and Swiss-US Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU and Switzerland to the U.S., respectively. Please visit the Privacy Shield Framework website to view our certification and [learn more about Privacy Shield](#).

Compliance with GDPR, which is effective as of May 25, 2018, is an active process and will continue up to and after the enforcement date. The GDPR provides a set of standardized data protection laws across all EU member countries, and is applicable to any organization collecting information from an individual residing in the EU regardless of where the organization is located. The European Commission does not currently offer GDPR certification. Please visit the European Commission website to [learn more about GDPR](#).

INDIVIDUAL RIGHTS

Individuals have personal data rights to the following:

- ✓ Be informed if personal data is being used
- ✓ Get copies of personal data
- ✓ Get personal data corrected
- ✓ Get personal data deleted
- ✓ Limit how organizations use personal data
- ✓ Portability of personal data
- ✓ Object to the use of personal data
- ✓ Decisions being made about an individual without human involvement
- ✓ Access information from a public body
- ✓ Raise a concern

SLEEP PROFILER PORTAL PRIVACY INFORMATION

The Sleep Profile software, which is accessed by the Sleep Profiler Portal (SP Portal), analyzes previously recorded physiological signals obtained during sleep with ABM's proprietary data acquisition systems. The software performs analyses of the acquired signals, presents the signals for editing, and delivers reports for the clinician. The software is fully compliant with regulatory guidelines (e.g., HIPAA, 21 CFR Part 11, etc.).

Collecting Information

There are several categories of information that ABM collects via the SP Portal:

1. Required information the user provides to utilize services
2. Other information the user provides to utilize services
3. Information we obtain to perform services
4. Technical support request
5. SP Portal access logs

The following provides detailed information regarding what type of data is collected and how long it is retained.

1. Required information the user provides

- a) SP Portal Setup Form

Each Commercial Customer designates SP Portal users who will have access to its SP Portal account. Personal information (i.e., name, credentials, username, email address, and phone number) for each user is provided to ABM as part of the SP Portal setup process. This information is associated with the Commercial Customer account.

- b) Patient Information

Information must be entered in the following fields to utilize the SP Portal services; however, the information may be pseudonymized, meaning the information entered can be coded by the user and does not have to identify a natural person. To keep an individual's health information anonymous to ABM, we recommend that users do not enter factual data.

- Name (first and last; middle name is optional)
- Date of Birth
- Gender

Personal information provided to ABM is saved to the SP Portal database, which is used primarily to provide technical assistance should any problems with a device, editing data, or generating a report be encountered.

2. Other information the user provides

Other information that may be provided for the purpose of enhancing our services. This information, which may be personally identifiable, includes:

- Patient Medical History Questionnaire
- Patient Sleep Diary
- Customer Profile (name, email, credentials, location data)

Other information may be provided to assist with the interpretation and analyzing of raw data obtained during sleep via ABM's proprietary data acquisition systems. This information, which is not personally identifiable, includes:

- Patient Information (patient ID, physician name and credentials, limited study information)
- Device Setup (settings and configurations)
- User Settings (download file location, device troubleshooting assistance, patient info location)

All information obtained is saved to the SP Portal database, which is primarily used to provide technical assistance should any problems with a device, editing data, or generating a report be encountered.

3. Information we obtain

When our services are utilized via the SP Portal, we obtain raw data from a ABM proprietary device. Once a sleep study has been recorded on a device, it is uploaded to the SP Portal. The user plugs the device into a USB port on their computer and the raw data is saved to a local drive to ensure that the upload, if interrupted, does not affect the integrity of the data. Upon being saved to a local drive, the user then transmits the raw data via the SP Portal for editing data and/or generating a report. Once the raw data file has been successfully uploaded to SP Portal, the user wipes the data on the device clean.

The Sleep Profiler software converts the raw data it received into a proprietary ".edf" file, which is identified only by a unique ID number assigned by the software and holds no patient-identifying information. Throughout the editing process only the unique ID number is associated with the .edf file. When the final report is being assembled, the software re-associates patient information with the final data, encrypts the report, and saves it on the SP Portal server. Reports are saved to the SP Portal server primarily to provide technical assistance should any problems with a device, editing data, or generating a report be encountered.

4. Technical support request

A user may request technical support by creating a ticket on the SP Portal. While no information is required, our Customer Representatives will be limited in assisting the requestor if personal data (i.e., name and either a phone number or email address) is not provided. All information included in a technical support ticket is initiated from support@advanced-sleep.com and is forwarded to ABM's Sleep Profiler's customer support team, who reaches out to the individual requesting assistance. The information is logged in a technical call spreadsheet to assist with customer follow-up and providing technical assistance.

5. Access Logs

ABM may automatically collect certain information and store it in log files when our services are utilized, including internet protocol (IP) addresses and a date/time stamp. This information is recorded in the database to administer services, analyze trends for service enhancements, and help protect ourselves from abusive users of our services.

Using Information

We use the information that you provide and we obtain to ensure that the SP Portal is providing value to our customers. Here are some of the ways that we do that:

- Provide technical assistance should any problems with a device, editing data, or generating a report be encountered
- Validate warranty coverage
- Communicate with customers, via email, regarding important improvements and enhancements to our devices and services
- Monitor types and trends of issues that are experienced when using the SP Portal for use in developing product and service enhancements
- Analyze usage and trends to publish de-identified findings for product marketing purposes and scientific journals
- Verify user identity and prevent fraud or other unauthorized or illegal activity.

Sharing Information

We do not sell, distribute, or lease personal information to third parties, ever.

COOKIES

The SP Portal only utilizes web server session cookies to identify the user once he/she has logged in, for the duration of the session. No personal data is saved. Cookies are small text files that can be used by websites to personalize a user's online experience and make the experience more efficient. Cookies are uniquely assigned to you and can only be read by a web server in the domain that issued the cookie to you. Cookies cannot be used to run programs or deliver viruses to your computer.

SECURITY

ABM is committed to ensuring that personal information is secure. We have physical, electronic, and procedural safeguards that comply with regulations to protect personal information. ABM uses industry-standard encryption technology to protect privacy. We limit access of personal information to employees who we believe reasonably need to come into contact with such information to provide products or services in order to do their jobs.

It is important for users to protect against unauthorized access to their device, computer, or SP Portal login information. It is the user's responsibility to sign off when finished using a shared computer or device. ABM will automatically log users off after 40 minutes of non-use.

For site security purposes and to ensure that this service remains available to all users, we use software programs to monitor traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. In the event of law enforcement investigations and as part of any required legal process, information from these sources may be used to help identify an individual.

DISCLOSURE

ABM does not sell, distribute, or lease personal information to third parties, ever.

ABM will disclose your personal information, without notice, if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on ABM or the site; (b) protect and define the rights or property of ABM; and (c) act under exigent circumstances to protect the personal safety of ABM website users, or the public.

RETENTION AND STORAGE

ABM retains personal information for no longer than necessary for the purpose for which it is processed. The length of time for which we retain information depends on the purposes for which we collected and use it.

All information is stored on secured servers owned and operated by ABM. We use third party vendors to support our services, which includes an IT Security Consultant. We store backups off site with third party storage provider to ensure data security in case of an emergency or catastrophe. All IT services are governed by a written contract.

ASSIGNMENT

If ABM is acquired by or merges with another entity, our assets, including all proprietary intellectual property and information embedded in our services and any personal information stored in our databases, will likely be transferred to the new entity. By utilizing our services you acknowledge and agree that ABM may assign assets and any information stored therein in the event of such a transaction.

CONTACT US

In addition to understanding what information we collect, how we use information, with whom we share it, and how long we retain it, as detailed above, individuals have other rights as identified in the "Individual Rights" section. Should an individual desire to exercise one of these rights, or have any questions regarding our privacy policy, please contact ABM by email at privacy-group@b-alert.com.