

# Privacy Disclosure for Sleep Profiler Portal

The Sleep Profiler portal electronically obtains, processes, and enables access to “protected health information” by a patient’s healthcare provider (“Provider”). Protected health information relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual. The privacy of this health information is protected by the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and by Advanced Brain Monitoring’s Privacy Shield Policy.

The Provider is responsible for: a) obtaining permission from the patient to enable storage of their health information on the Sleep Profiler servers, b) utilize the software features designed to limit access to the protected health information, and c) notify Advanced Brain Monitoring if/when patient data must be deleted from the servers (i.e., patient opt-out).

Advanced Brain Monitoring’s policies with respect to a) protection of patient privacy, b) administrative, physical, and technical security safeguards, and c) for protection for a potential loss of data are defined below.

## Protection of Patient Privacy.

- Protected Health Information (PHI): ABM may use or disclose PHI to perform functions, activities, and/or services for, or on behalf of, its Clients, provided that such use or disclosure does not violate Privacy Rules (e.g., HIPAA regulations), or additional requirements explicitly requested by the Client. All ABM employees, agents, and subcontractors that create, receive, maintain, or transmit PHI on behalf of ABM shall apply the same restrictions, conditions, and requirements to ensure protection of said PHI.
- Breach Reporting: ABM will report in writing to its Client, within two (2) business days after discovery, any suspected or actual: (a) access, use, or non-permitted disclosure of PHI; (b) breach of unsecured PHI in accordance with 45 CFR 164.410; (c) security breach or intrusion; (d) use or disclosure of PHI in violation of any applicable U.S. federal or state laws or regulations.

## Compliance.

- SQL Server 2012 is used for the database servers. Secure SSL protocol (2048-bit) is used to encrypt when transferring data over the internet. Patient names associated with other PHI stored in the database are encrypted at rest.
- Primary servers in San Diego, CA and mirrored backup servers in Phoenix, AZ are at secure SOC 1/SSAE-16 certified facilities with 24-hrs/day x 7-days/week staffing, biometric and physical electronic card access, locked cabinets, redundant power, and internet diversity with over 6 different providers.
- Firewall and router protection with Distributed Denial of Service recognition capability to secure inbound connections from/to Internet with intrusion protection, antivirus/antispysware, and ongoing logging via firewall router.
- Controlled access to servers containing patient data with monitoring and logging of all administrative level access to servers which contain PHI.

## Disaster Recovery.

- The primary servers employ Raid-6 arrays to allow for failure of multiple drives without impacting availability of data.
- Point-in-time snapshots /backups of the data are taken at multiple points per day to provide recovery of any of the servers.
- The primary servers are replicated every 15-minutes to identical secondary servers located in Arizona.
- Snapshots via Hyper-V Replication are generated hourly and retained for 6-hours. Local VVS snapshots are taken 3 times per day and retained for up to 60 days. Full backup recovery points are taken twice per day and retained for 30 days.

## Ownership of Data.

While ABM claims no ownership rights with respect to PHI, all users of the Sleep Profiler Portal grant ABM the right to aggregate Sleep Profiler de-identified data on its servers so long as PHI is not disclosed and de-identified data aggregation is related to system improvements, research related to improvement of methods of payment or coverage policies, and publication relative to patient populations that may benefit the scientific community and improve patient care.