



Technical Information, Security Features, and HIPAA and FERPA Compliance

This document outlines the technical details for system requirements, security features, and compliance information for the AEPS[®]i system for use with AEPS[®]-3 located at www.aepsi3.com.

ABOUT AEPSI FOR AEPS-3

AEPSi for AEPS-3 is an Internet-based application, hosted on Brookes Publishing Company's servers in Ashburn, VA with a fully managed hosting company, Rackspace.

AEPSi uses PostgreSQL for the database and Elixir for the application.

REQUIREMENTS

Each user computer must have the following:

- Any PC or Mac computer with the most up-to-date operating system, with one of the following browsers: Google Chrome, Mozilla Firefox, Safari, Microsoft Edge.
- Browser must be configured to accept cookies.
- Browser must have JavaScript enabled.
- To view and print reports, questionnaires, and other documents, the free Adobe Acrobat Reader[®] (<http://get.adobe.com/reader/>) is required.
- AEPSi can be accessed on mobile devices with a secure internet connection.

SECURITY

Overview

Brookes Publishing Co., the publisher of AEPSi, is committed to keeping your data safe, secure, and private. AEPSi uses robust security measures and employs the appropriate physical and technical safeguards to protect user data, child data, and other data entered by users in the AEPSi system and ensure over time their continued confidentiality and correct use.

Our fully managed hosting company, Rackspace, is SOC/ISO/IEC 27001:2005 certified, one of the most widely recognized auditing standards for service companies. Rackspace reached this level of recognition for its reliability, security, and ability to safeguard IT operations. We protect your information with industry standard Internet security measures. When you use our secure online services, we protect your data in a secure, restricted-access environment. Your account information or specific assessment data remain yours and cannot be shared with any third party without your prior approval.

Network Security

Browser-level encryption protects all of your confidential data and information. AEPSi uses SHA-256 Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption, which is also employed by most financial institutions, medical data centers, and government agencies to ensure that data are secure from interception during transmission. To authorize and certify access, we use VeriSign, an advanced security solution designed to provide secure communications and transactions over the Internet and private networks. SSL prevents unauthorized access to your data.

Access Security

Our servers are protected by industry standard firewall technology. Only authorized traffic and requests from legitimate sources are allowed through our firewalls to ensure the safety of both user's data and our server equipment.

Data Security

Your information is stored on secure data centers, which use redundancy to protect against data loss and are designed to recover data quickly in the event of a hardware or disk failure. Brookes Publishing takes precautions to protect the confidentiality and security of the data collected and stored in the site's database by using industry-recognized security safeguards such as firewalls, coupled with carefully developed security procedures to protect your information from loss, misuse, or unauthorized alteration.

Regular backups of the site and all data are made; all data are backed up in full on a weekly basis, with incremental backups being made daily. Backed-up data are stored at a secure site for a period of 90 days.

Physical Security

Our databases and the servers on which we store site information are kept in a secure data center that includes physical security, conditioned power, environmental controls, uninterruptible power supplies, diesel generator, and fire suppression technologies.

Password Security

Users can only gain access to the system by providing a valid username and password combination, which is encrypted while in transmission. Password-protected information is only available to you or authorized users within your organization. No access is allowed to the site without a valid username and password combination. A username must be unique across the entire AEPSi system, not just within a particular account. User passwords must have a minimum length and are encrypted using a read-only method so they cannot be viewed or decrypted from the database.

COMPLIANCE

HIPAA Compliance

If you are a “covered entity” as that term is defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) implementing regulations with regard to the Standards for Privacy of Individually Identifiable Health Information, Brookes is prepared to become your Business Associate, as defined by HIPAA, when you are an AEPSi subscriber. Upon submission of your desired template for your Business Associate Agreement, Brookes shall, upon review and acceptance, commit in writing to the mandatory provisions in HIPAA regarding the use and disclosure of protected health information, as the terms “use,” “disclosure,” and “protected health information” are defined in HIPAA in the Privacy Rule. We provide a secure online environment to protect the privacy of our AEPSi subscribers and their users, as described above.

FERPA Compliance

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. This law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. If this law applies to your organization and you are an AEPSi Authorized User, you must be aware of your obligations under this law and respect its terms. AEPSi provides a secure environment in which you can be sure you are complying with FERPA if necessary.

For more information, [contact your sales representative](#) or call 1-800-638-3775.