Application and Data Security Briefing

The following is a summary of the basic approaches and measures taken by EAB to safeguard data, and is not a comprehensive representation of the procedures or protocols.

Transmission of Data
EAB requires the secure transmission of member data to and from our network; we work with members to discourage transmission that is otherwise not secure. This is accomplished through a combination of Transport Layer Security (HTTPS) protocols, SSL certificates, and data encryption. Upon receipt, source files are logically separated and isolated from other members.

Data Storage and Security
All member data (source file and application) are stored in a certified data center in the U.S. that is co-managed by the Advisory Board Company and the hosting provider. In addition to HIPAA attestation, the provider’s data center compliance program includes FISMA moderate attestation, PCI DSS 2.0 validation, SSAE 16 Type 2 SOC 1, SOC 2 Type 2 examination, U.S.-EU Safe Harbor certification, LEED Gold certification, and the EPA ENERGY STAR certification. Access to the data center is controlled by role and granted by explicit business need. Application data is partitioned by unique member identifier at the database level. Member data can only be accessed by authorized users assigned to this member ID.

Data Backup and Recovery
EAB maintains an updated disaster recovery plan. All production database servers are backed up regularly, with full weekly and daily incremental backups occurring. All production application build code is backed up nightly. Local backups are replicated to tape in encrypted format. Tapes are transferred to a secure offsite facility daily.

Application Security
For non-SSO members, the web interface provides industry-standard password controls (length, complexity, aging) and multi-factor authentication. For all members, the web interface is accessed via always-on HTTPS.

Security and Penetration Testing
SSC has had penetration testing performed by Secure Ideas LLC, an independent security consultant. This security audit found that SSC and its infrastructure “are adequately protected with the appropriate controls and are based on industry information security standards and regulations.”

Physical Security
All employee laptops and portable USB drives employ industry-standard full disk encryption. Physical access to EAB facilities is limited through picture IDs and proximity cards.

Safe Handling
All employees with access to member data must pass thorough background screening and go through regular security/privacy training. EAB also employs industry-standard technology to mask/remove PHI data from non essential/production environments.

Usage of Data in Non-Production Purposes
Core to the Collaborative, EAB will periodically conduct research analysis projects against the aggregated data from our members. For these activities, all data is masked to remove any identifiable information.

FERPA Compliance
To the extent that EAB receives or otherwise has access to personally identifiable information from a student education record, EAB maintains these records in accordance with the requirements of the Family Educational Rights and Privacy Act, 20 USC § 1232g, and its implementing regulations, 34 CFR pt. 99, as each may be amended from time to time.

Single Sign-On
EAB currently supports single sign-on with CAS, AD/LDAP, and SP-initiated Shibboleth, given that the SSO is already setup and configured on the institution infrastructure. Members with a set up and configured SSO can switch from the standard SSC registration process to single sign-on at any time. SSC is a member of the InCommon Federation.