ePath Learning ASAP Technical Requirements Overview: 21CFR Part 11

ePath Learning supports FDA 21 CFR Part 11 technical compliance requirements for organizations in FDA regulated industries. Title 21 CFR Part 11 requires companies to implement controls, including data security, system validations, audit trails, electronic signatures, and documentation for software and systems that are involved in processing electronic data, as part of their business practices and product development. The table below provides an overview of ASAP's technical control features as well as ePath Learning's internal control processes.

ASAP LMS Technical Controls

Verification	• Electronic signatures
Access Control and Encryption	• Authentication is based on user ID, password and time of day. • Authorization control is based on roles and access permission lists. • SSL network encryption. • Symmetrical strong data encryption for passwords. • Client data is isolated by University. • Learners' history is not accessible directly and is updated based on actions by the learner or an authorized action by a builder.
Audit Trails	• All actions related to learner's history are audited. • The audit trail cannot be changed by learners or builders. • Each event has a system generated time-stamp. • Reports provide detailed description of learners' history transactions and the origin of the data. The data in the reports cannot be changed by users.
Database Integrity and Abstraction	• The database cannot be accessed directly by users. • The system employs an Oracle database and supports full RDBMS ACID compliant transactions.
Application Validation and Staff Training	• Regular security orientation and training of technical and engineering staff. • Ongoing validation of software releases and software updates against a comprehensive security test plan. • Regular audits and penetration tests of core functions to ensure each function is performing as expected. • Peer reviews of critical system functions to ensure adherence to proper authentication, authorization and encryption controls. • Separation of engineering audit from QA audit to ensure proper delineation of accountability and test results.