ePath Learning nGage™ Technical Requirements Overview: 21 CFR 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 nGage's technical control features as well as ePath Learning's internal control processes.

Verification	• Electronic Signatures
Access Control and Encryption	• Authentication is based on user ID, password, and organization code. • Authorization control is based on roles and access permission lists. • Communication with the platform is over HTTPS, using TLS 1.2 for encryption. • Encryption of passwords using BCrypt key, a one-way hash utilizing 128-bit salt and 192-bit hash value. • Customer data is isolated by system Client. • Users' history is not accessible directly and is updated based on actions by the user or an authorized action by an administrator.
Audit Trails	• All actions related to user's history are audited. • The audit trail cannot be changed by users or administrators. • Each event has a system generated time-stamp. • Reports provide detailed description of users' history transactions and the origin of the data. The data in the reports cannot be changed by users.

ePath Learning | 300 State Street Suite 400 | New London | CT 06320
860.444.7900 | www.ePathLearning.com

Database Integrity and Abstraction	• The database cannot be accessed directly by users. • The only public access to customer information on our servers is provided by our web servers, located behind AWS Elastic Load Balancer. All requests for client data are checked for proper authentication and authorization. • All nGage authentication and authorization failures area logged. Repeated authentication or authorization failures are flagged and monitored. • The system utilizes AWS S3 for file storage and RDS for managed PostgreSQL database servers.
Application Validation and Staff Training	• Regular security orientation and training of technical and engineering staff. • Documented Software Development Life-cycle (SDLC). • Ongoing validation of software releases and software updates against a comprehensive software 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.