685 Route 202/206
Bridgewater, NJ 08807
www.repligen.com

PATsmart™ REBEL® System and 21 CFR Part 11 Compliance

21 CFR Part 11 ('Part 11') establishes FDA regulations on an organization's handling, storage and management of electronic records & electronic signatures (ERES) to ensure equivalency to paper records and signatures.

This technical note describes PATsmart™ REBEL® System's support for operation in a 21 CFR Part 11 compliant environment, with its integrated support for data integrity measures, access controls, and system audit logs.

Product Development

Software Development Process

Repligen uses industry standard development practices, including full source and revision control (Git), and a dedicated software quality assurance team with documented test scripts and outcomes. Software features, improvements and bugs are documented in Jira (Atlassian Software), and code traceability is provided via Bitbucket (Atlassian Software). Software builds are automated on controlled build management VM's using Team City (Jetbrains). Release notes are published when software updates are made available to customers / administrators.

Product Development Process

Repligen uses a defined product development process as defined in its ISO 9001 Quality Manual. This phase-gate process moves products from concept to production through the following formal review gates: preliminary design review, critical design review, system qualification review, and test readiness review. The contents of these gates reviews, attendees, minutes are archived in our requirement management software. Product specification documents in the form of a user requirements document, and system requirements document are formulated and traced in JAMA Connect (JAMA Software), along with a Requirements Verification and Traceability Matrix and test verification. Defects/failures in the development process are captured in electronic task tracking systems including Jira and Trello.

Manufacturer Quality Systems

Repligen is ISO 9001:2015 certified. ISO 9001:2015 certification specifies requirements for quality management systems designed to ensure customers consistently receive high-quality products and services. This includes structured and documented procedures for product design, manufacturing and customer support. The focus on effective management systems, continuous product improvement and customer satisfaction are all critical components of Repligen's business.

REPLIGEN

685 Route 202/206
Bridgewater, NJ 08807
www.repligen.com

REBEL SYSTEM Product Attributes

Identity Management

Access to REBEL System functions are protected by username/password access controls at the individual user level. Site specific policies for password lengths or complexity, or expiration should be imposed by secondary policies/procedures. The REBEL System prevents the creation of duplicate accounts, and accounts with blank passwords.

Access Controls

Access to REBEL System functions are protected by username/password access controls at the individual user level. Two user levels are available: user and administrator. User-level operators have access to core system functions to run samples, but no access to modify system settings. Administrator-level operators have access to all functions, including core system functions and system settings. The system will automatically logout the current user if the system has been left inactive for up to 30 minutes.

REBEL System's data and reports can either be stored on internal storage, or on a network share. Secondary policies/procedures should be implemented to ensure the integrity of REBEL System data and reports stored on network shares outside of REBEL System's controls.

Electronic Signatures

As an automated sample analysis system, REBEL System is designed to acquire data and perform a quantitative analysis of samples placed in an autosampler queue. As such, electronic signatures associated with creation, analysis, results, reporting and review should be performed in a secondary review system. REBEL System's report formats are selectable as CSV or PDF (for easy import into e-LIMS or e-Notebook platforms). Reports created at the origin in REBEL System do list the username of the party responsible for the samples. This may be acceptable for 'creation' identification depending on your organizations policies.

Audit Trails

The REBEL System records and timestamps all critical system actions such as user logins/logouts, password changes, system modifications, completion of assays, and completion of system regular maintenance and performance qualifications. These audit log files are automatically exported in human readable form to the system's configured network location in real-time. Secondary policies/procedures should be implemented to ensure the integrity of the audit log files once located on network shares outside of REBEL System's control.

685 Route 202/206
Bridgewater, NJ 08807
www.repligen.com

Records Retention

When configured for Network storage, the REBEL System saves raw data files, and reports (CSV or PDF) on the designated network share in real time. No permanent storage of raw data files or reports is ensured on the REBEL System internal storage system. It is expected that a company's corporate IT policies can be employed for the resulting files deposited on network shares for long term retention, fraud prevention and adulteration.

We recommend that interested parties review the REBEL System Network Overview guide for additional details on the network topologies supported by the REBEL-embedded software.