LabLog®

Lab Notes. The Clever Way.

STRATEGIES FOR LIFE SCIENCES COMPANIES USING **LABLOG** WITH **GXP SYSTEMS**

Authors: John Himes, Hani Ebrahimi

Reviewers:
LabLog: Pamela Gallagher, Elizabeth Proctor
Industry: Ashley Orillion (The Janssen Pharmaceutical Companies of Johnson & Johnson), Edward Worthington (ESafetySystems), Danny Chadha (VitalCompliance), Anil Saldanha (SeamlessTrust)

INTRODUCTION

An increasing number of biotechnology and pharmaceutical businesses are embracing modern technological advances in cloud computing and data storage in an effort to reduce costs and increase profit margins. By leveraging unlimited computing and storage resources in the cloud, organizations of all sizes are undergoing digital transformations. This reduces IT investments and positively impacts revenue.

Unlike most businesses, however, biotech and pharmaceutical companies must balance the advantages of modern computing technologies with strict regulatory requirements. For instance, effectively responding to audit requests can be challenging when coupled with rapidly changing technologies.

The regulation most relevant to life sciences companies is the United States Food and Drug Administration's (FDA) Title 21 CFR part 11. This set of regulations applies to companies that manufacture chemicals, drugs, and medical devices for use in the United States. The requirements of Title 21 CFR Part 11 cover computer hardware and software systems designated for digital document storage. The FDA expects that all digital documents maintained under this part will be readily available for inspection [Ref: 21 CFR Part 11, section 11.1 (e)].

Since its conception in 1999, Title 21 CFR Part 11 has been enforced with increasing intensity. The FDA reports many deviations to this regulation. In fact, three in ten electronic record inspections fail, according to the FDA's presentation at the 31st International cGMP conference in Athens, GA [Ref: https://www.labcompliance.com/solutions/expert_advice/computers/4104-warning-letters-part11.aspx accessed August 12 2019].

The FDA's warning letters and Inspectional Observations (FDA Form 483) highlight a range of software-related topics including insufficient data security with an inability to overwrite data, lack of computer validation, invalidated off-the-shelf software, inadequate storage and back-up, unvalidated databases, unsaved electronic raw data, failure to conduct formal risk analysis after changing software, and changing electronic data after its approval by the supervisor.

At LabLog, we continually perform in-house and external validation of our systems against the latest regulations and security standards. This is in line with our goal to create a software that simplifies laboratory record management in highly regulated environments. A robust information security strategy is essential for meeting the FDA's requirements for computerized laboratory records. In this whitepaper we explain how LabLog leverages modern cloud technologies for comprehensive information security in the context of Title 21 CFR Part 11 and other GxP guidelines.

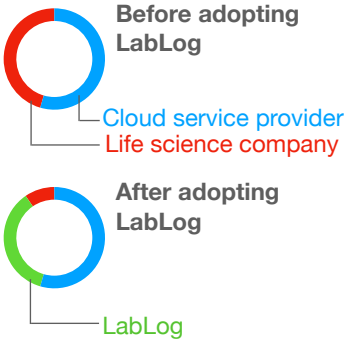
ABOUT THIS WHITEPAPER

LabLog's mission is to protect your data and make sure that it's always available to you. Our philosophy necessitates data security, resilience, and availability. In this document you will learn how we technically achieve these expectations and how we leverage Microsoft services and external audits to perform independent tests against accepted international standards for cybersecurity and service trust including Title 21 CFR Part 11.

This paper will help life sciences companies to:

- Analyze the data security requirements of Title 21 CFR Part 11.
- Define how LabLog can meet those requirements.
- Define the levels of shared responsibilities for compliance to Title 21 CFR Part 11, when adopting LabLog (Figure 1).

Fig. 1. **Reduced responsibilities by adopting LabLog.** Charts show ratio of shared responsibilities for 21 CFR Part 11 compliance.



The Importance of IT Security

Lapsed data security measures and unvalidated record management software has lead to the demise of companies manufacturing therapeutic products. At best, a poorly implemented software solution leads to substantially higher costs and diverts resources in response to FDA and CMS inquiries.

Though referred to as 'data in the cloud,' all data is stored inside data centers across the globe. These locations are vulnerable to technical failures including power outages and system corruption. While redundancy mitigates risks to availability, a system's integrity and confidentiality are also top priorities. It is therefore critical to implement the proper countermeasures to prevent hacking, un-authorized access, and foreign government interference. LabLog's analysis shows that the majority of Electronic Laboratory Notebook (ELN) providers are not transparent about their data storage practices and leave their data vulnerable to loss and compromise. At LabLog, we leverage Microsoft Azure data centers located within the United States to provide full redundancy via secondary backup sites. All client data flowing into LabLog is backed up in real time. In addition, read and write operations are performed at independent data centers to minimize the likelihood of corruption. By only storing data in facilities located in United States, we meet the highest privacy standards. In fact, the Azure data centers that host LabLog are located in the same geographical location as the Azure data centers that host the federal government's highly sensitive information [Ref: https://azure.microsoft.com/en-us/global-infrastructure/government]. Since the concept of our company, LabLog's primary concerns have always been data security and readily available data that research teams need.

Cloud Services in Regulated Healthcare Environments

Organizations across all industries are implementing cloud services as part of their digital transformations, yet this shift comes with unique challenges for the life sciences sector. These businesses want to take advantage of the improved redundancy and lower costs of cloud computing, but they need to balance these needs with their industry's strict regulations to ensure the safety of products and patients.

These considerations are especially crucial for new biotech companies who are still establishing their Quality Systems and planning to submit applications for FDA review. Whenever we create, move, or store data, we must ensure that we take the necessary steps for the above stated principles.

After extensive research, LabLog's development team decided to leverage Microsoft Azure for GxP cloud computing. Microsoft Azure is an established cloud service provider that already works with numerous life science businesses. Azure, therefore, has streamlined compliance and auditing procedures, simplifying the compliance pathway for LabLog and our clients.

In addition to Title 21 CFR Part 11, another key regulation for life sciences companies is Title 21 CFR Part 820, which concerns purchasing controls for IT systems and relationships between vendors and cloud service providers. The fundamental goal of the FDA regulations and other applicable GxP guidelines is to ensure product and patient safety. The following table

summarizes the set of LabLog's built-in features designed to meet the relevant requirements of the above mentioned regulations:

REQUIREMENTS	HOW LABLOG MEETS REQUIREMENTS
Data Integrity (part 1) **Electronic Signatures.**	LabLog has built-in features for managing and using electronic signatures. Users with pre-defined roles can sign documents for approval and review. Approved documents cannot be modified.
Data Integrity (part 2) **Security to safeguard systems.**	At the application level, LabLog restricts access based on pre-defined user roles and organizational hierarchy. At the system level, LabLog adheres to standards defined by Microsoft and ISO27001 to protect against internal and external threats.
Data Retention **Documents shall be available for audit by FDA during a product's life cycle.**	LabLog offers a rich set of features for audit-trail management. The data retention period is determined by individual organizations, and it can vary from two to 15 years.
Backup and recovery **Have robust disaster recovery in place for both data center and service.**	By leveraging Microsoft Azure cloud services, LabLog implements a robust backup and recovery system.

Defining Compliance Standards for IT Security in Life Science Research and Development

Title 21 CFR Part 11 sets a minimum benchmark for IT security. This benchmark includes encryption standards for data sent over the internet. It also sets guidelines for access control and signature management. LabLog meets and exceeds these requirements by adhering to two additional standards, namely SOC TSC and ISO27001. At LabLog, we request third-party assessment of our systems for independent verification, and all documentation is available for our clients to facilitate compliance with Title 21 CFR Parts 11 and 820.

SOC TSC

The American Institute of Certified Public Accountants (AICPA) developed Service Organization Control's Trust Services Criteria (SOC TSC) for use in consulting arrangements to assess IT systems. The TSC assessment entails data security and availability, processing integrity, confidentiality, and privacy [Ref: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html].

ISO 27001

Created in collaboration by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the ISO 27001 is an information security management system (ISMS). This set of policies and procedures includes technical, physical, and administrative controls that guide information risk management processes. While Title 21 CFR Part 11 provides specific controls and guidelines and the SOC TSC gives us another way to standardize and audit those controls, ISO 27001 details an organization's overall risk-management strategy. It also provides an auditable framework for high-level security planning and management.

In summary, by combining Title 21 CFR Part 11 with SOC TSC and ISO27001, LabLog curates a layered defense in-depth strategy that prioritizes data confidentiality, integrity, and availability. We allocate more resources to building controls and conducting audits because we understand the true value of data.

Building LabLog on Microsoft Azure

Microsoft Azure is a cloud computing service that provides on-demand computing resources for organizations seeking access to a scalable, secure, and immediately accessible platform. Many life sciences organizations use this IT solution for hosting GxP-regulated systems due to Microsoft's Trusted Cloud Initiative, which promises security, compliance, transparency, and privacy [Ref: https://www.microsoft.com/en-us/trust-center#Trusted-Cloud-initiative]. Azure data centers located exclusively within the United States host all of LabLog's backend services. This includes LabLog's primary and backup-secondary servers, databases, and file storage services.

Microsoft dedicates tremendous resources to maintaining a multi-layered approach to securing its Azure cloud platform. By leveraging the Azure platform, LabLog benefits from Microsoft's teams of dedicated IT professionals who track and combat emerging threats to protect data from unauthorized access and alteration. LabLog also benefits from Azure's

integrated solutions that leverage AI to assess and manage compliance risks. We detail Microsoft Azure's compliance with both FDA 21 CFR 11 and ISO 27001 below. By making their reports easily available, Microsoft empowers LabLog and its users to access, download, and share relevant reports. Furthermore, Azure enables senior management at LabLog to view the results of the automated audits performed on LabLog's systems.

Independent Verification of Compliance

For independent verification, Microsoft requests third-party specialized teams such as Accenture Life Sciences to conduct assessments of their services. Accenture Life Sciences has concluded "that the security design, procedural controls, and tools of Microsoft Azure meet the standards of the life sciences industry." We likewise trust Microsoft Azure's capabilities to secure our data and maintain compliance standards. At LabLog we also require third-party verification of our systems. First, Azure's AI capable tools perform automated audits on LabLog's cloud systems to ensure compliance to the latest security standards. Second, a third-party specialized team assesses and certifies LabLog's compliance.

Shared Responsibilities for FDA 21 CFR 11 Compliance

Microsoft Azure GxP Guidelines (Appendix C) highlights the sections of Title 21 CFR Part 11 that fall under Microsoft Azure's responsibility [Ref: https://gallery.technet.microsoft.com/azure-gxp-guidelines-ab1b98d9]. A typical agreement with LabLog covers the following support and maintenance functions:

1. Generation of accurate and complete copies of records (data and associated metadata) in human readable form. Responsible parties: LabLog and individual organizations.
2. Protection of records to enable accurate and ready retrieval throughout the records retention period. Responsible parties: Microsoft and LabLog.
3. User access controls to limit system access to authorized individuals. Responsible parties: Microsoft, LabLog, and individual organizations.
4. Secure, computer-generated, time-stamped audit trails to independently record the date and time of user actions that create, modify, or delete electronic records. Responsible parties: Microsoft and LabLog.
5. Enforcement of permitted sequencing of steps and events, as necessary. Responsible party: LabLog.
6. Data input validity verification, as necessary. Responsible party: LabLog.
7. Encryption of data at rest and in transit. Responsible parties: Microsoft and LabLog.
8. Identify clear roles and responsibilities for LabLog's cloud environment. Responsible party: LabLog.
9. Establish governance policies and procedures that are aligned to the cloud model. Responsible party: LabLog.

While Microsoft provides the foundational IT security that allow LabLog to maintain compliance with FDA

regulations, other responsibilities fall to LabLog. Most life sciences companies, whether or not they use a different ELN solution, have had to bear this burden alone. LabLog's mission to empower researchers helps us identify areas where we can assume some of these duties. LabLog therefore reduces the burden on individual client organizations.

There remain some responsibilities that fall solely under the individual organizations. These include:

1. Train responsible personnel in using LabLog.
2. Manage relationships with LabLog and review service agreements.
3. Identify cloud resources and services, including LabLog, using a standardized naming convention to support system inventory and documentation.
4. Plan validation of LabLog with key stakeholders.
5. Perform routine monitoring to verify service quality.
6. Establish continuous improvement activities in coordination with LabLog.

LabLog's Responsibilities

Personnel training

At LabLog, we require our technical team to go through comprehensive security checks and training. Plus, we mandate security training as part of our onboarding process, and we require that employees attend regular workshops.

Managing supplier relationships

The LabLog team takes responsibility for managing supplier relationships with Microsoft Azure. We handle the entire infrastructure pipeline, including all the paperwork.

Data backup and restoration

We have implemented a robust data backup and restoration process. Our geo-replication approach stores all data on two independent geographical locations. One is at a primary data center in the central US and a secondary one is in the eastern US. This protects against hardware failures, network or power outages, and natural disasters. By allowing us to easily fail-over all our systems and data from one location to the other, we ensure a smooth restoration process. Altogether, these systems give us extra layers of redundancy, which allows us to guarantee 99.999% availability.

Routine monitoring and testing

We regularly conduct audits using Microsoft's automated tools and other third-party accreditors. A copy of the most up-to-date reports can be requested by contacting the LabLog support team.

Data integrity

Data integrity is one of the defining principles that governs the specifics outlined in Title 21 CFR Part 11. LabLog implements cryptography and best security practices for data at rest and data in transit. We use AES to encrypt all incoming user data. A set of private encryption keys are required for inflight decryption of all user-requested outgoing data. All encryption keys are stored in the Azure Key Vault and accessible only to the LabLog's API, which runs on our production servers. This allows our development team to improve and maintain LabLog and its underlying

systems without accessing encrypted user data.

Audit trails

LabLog captures the following information for the generation of audit trails:

- User information, including user id, name, and email (masked for security)
- Action names such as create, update, delete
- The IP address of the client system
- Time-stamps
- Authentication modes
- Metadata for documents created and modified by users

Activity logs are stored independently from user generated content. LabLog uses the stored logs to create human-readable audit logs as required for internal or FDA review.

We strive to make FDA compliance and other security issues as simple as possible. However, ultimate responsibility rests with individual organizations. It is essential that organizations identify clear roles and responsibilities for team leaders and members. LabLog's built-in tools allow creation of various compliance-based roles, such as reviewer and approver.

Furthermore, it's crucial that organizations establish governance policies and procedures. This includes restricting access to authorized personnel, monitoring and controlling user privileges, and hardening devices by following a regular patching schedule, disabling unused ports, and similar measures.

Training and raising awareness are also fundamental components of defense for compliance adherence. It's important that all employees—not only those who work in IT or security—understand risk management and mitigation. This includes raising awareness against social engineering attacks like phishing. It's important to include this training as part of the hiring process and to conduct regular sessions, especially considering the ever-evolving threat landscape.

CONCLUSION

IT security is a major challenge for any 21st century enterprise. As hackers develop more sophisticated methods, the potential for causing destruction rises with our increased dependency on digital infrastructure. Therefore, staying ahead in the cyber arms-race is a top priority. LabLog understands your need for secure systems, reliable software, and high uptime, but we also recognize the importance of user experience and convenience.

Partnering with Microsoft and utilizing their Azure cloud infrastructure has enabled us to provide world-class computing at a fraction of the cost compared to an independent software. We then took it one step further by implementing systems that are tailored to the highly regulated pharmaceutical and biotechnology industries.

We designed LabLog for Title 21 CFR Part 11 compliance from the ground up. We have immense respect for researchers and the work that goes into generating quality data for regulatory approval. Thus, we strive to provide an exceptional ELN solution. We're constantly improving in the attempt to strike the perfect balance between convenient features, user accessibility, and security and compliance concerns.

STAY CONNECTED

www.linkedin.com/
company/lablog

@lab_log

VISIT OUR BLOG

labnotebook.app/blog/