



## **In-House vs. SaaS-Hosted LIMS Security**

**10 Reasons Why LIMS is More Secure in a Sciformatix SaaS-Hosted Environment**

## Introduction

Software as a Service (SaaS) is quickly becoming the standard delivery model for many forms of software applications, including critical IT software (e.g., email, collaboration software, etc.) and business applications (e.g., CRM, human resource management, etc.). And, now, Laboratory Information Management System (LIMS) solutions are available via SaaS from Sciformatix. Organizations realize many benefits by leveraging SaaS services. The On-Demand model of SaaS infrastructure provides benefits to the customer by lowering their startup expenses and overall costs, while increasing flexibility, reliability, and overall solution security. However, as new organizations begin to evaluate SaaS software and services, many still have concerns about security, fearing that hosting their critical applications and data with a SaaS provider will expose them to greater risk and loss of control.

This concern is particularly acute for the needs surrounding the management of information for a scientific lab, specifically as it relates to LIMS. For non-sensitive information maintained in a LIMS, security concerns may not be significant; however, where sensitive information is involved, the security of that information is of utmost importance.

This whitepaper compares the security provisions for a common in-house LIMS deployment versus a cloud-based model with Sciformatix as the SaaS provider. By choosing Sciformatix as their SaaS LIMS provider, scientific labs can achieve superior data security for their sensitive information over in-house implementations, providing the peace of mind that is necessary for many scientific endeavors.

---

## The Importance of LIMS and LIMS Security

Scientific labs have become increasingly dependent upon information technology to track lab information, manage lab processes, and capture experimental results. A lab may produce hundreds, thousands, or even millions of data elements that need to be captured, managed, and made available for future examination. This information may include details about samples and their locations, subject (patient) characteristics, usage and measurements, experimental conditions, and many other forms of information.

Why are Laboratory Information Management Systems (LIMS) popular and necessary? First, reliably tracking the abundance of lab information, even for small labs, is no small problem, considering that a lab may have hundreds, thousands, or even tens of thousands of samples and other material in their inventory, and details must be captured about lab operators, processes, material usage, and other information. Second, the introduction of bad data or transcription errors via manual processes can lead to significant problems for a lab. Third, insufficient record keeping and a lack of trace-back can lead to regulatory and/or internal compliance issues, particularly given ever-increasing standards such as Sarbanes Oxley, HIPAA, HCFA, GxP, CLIA, and others. And fourth, the lack of automation forces humans to do work that can be performed much more efficiently and accurately by computers.

In the early stages of a lab's activities, it is common to utilize Excel spreadsheets to capture and manage lab information. Over time, labs often recognize the need to improve their information systems and raise the productivity of lab workers, taking the step towards a more comprehensive LIMS. Some labs embark on an in-house development effort, often utilizing somewhat informal tools such as Microsoft Access or FileMaker Pro as their development and operating platform. Others choose to acquire a solution from a commercial LIMS provider. In both cases, the most common deployment method has been to install and run the LIMS software on in-house computer systems.

Why is LIMS security important? The information stored in a LIMS may be sensitive for one of two reasons: 1) Patient information may be included, and privacy rights must be respected; and 2) The information may be proprietary to the lab and/or its parent company or partners, helping to provide a business or scientific edge over competitors. Leaking patient information is bad public policy and may lead to legal and monetary issues for a lab. Leaking proprietary business and/or scientific information can lead to legal issues and/or negatively impact the operations and competitiveness of a lab. Therefore, it is easy to see why maintaining effective security for LIMS is important for the business of a lab.

---

## The 7 Layers of Security for a “Secure” In-House LIMS

While LIMS are incredibly useful and productive, they can be vulnerable to different types of threats. A comprehensive security strategy protects against these important threats:

- Viruses and malware – Attackers who plant a virus or malware that can detect database instances and connection strings, striving to invade a database for nefarious reasons, such as deleting a database or corrupting valuable data.
- Employee negligence and/or malicious employees – Employees, ex-employees, or contractors who inadvertently compromise sensitive business information, or worse, purposely try to access and/or steal privileged information.
- Corporate espionage – Attempts by competitors to gain an unfair advantage by accessing internal information including project details, sample data, lab processes, experimental results, and other valuable scientific data.
- Hackers – Pirates looking for valuable information that they can either use to illegally profit or sell on the “black” market.

Does your lab organization properly secure your LIMS and other information systems against these threats, employing a multi-tiered security infrastructure? Security should span multiple layers:

### **Layer 1: Physical Security**

Most small and medium sized lab organizations that host their own LIMS servers do so out of a corporate office or within the lab. Servers are typically kept in a server closet or computer area, often protected by just a single locked door. While businesses often feel more comfortable keeping servers within eyesight inside their own offices, their trust may be misplaced. Every year, thousands of businesses experience theft, burglary or trespass, resulting in the damage or loss of computer hardware and ultimately their LIMS servers.

### **Layer 2: Logical Server Security**

LIMS data is only as secure as the servers it resides on. To properly secure LIMS data, the LIMS servers must be properly secured. This complicated, continuous process includes:

- Proper operating system installation and hardening configuration
- Prompt testing and installation of security patches and updates to the operating system
- Strict configuration of user and administrative accounts with roles and permissions
- Proactive monitoring of the servers for viruses, intrusions, and any unexpected behaviors such as Denial-of-Service (DoS) attacks and intrusion attempts.

Unfortunately, most small and medium sized lab organizations do not have the necessary experience or resources to allocate towards these tasks, thus creating exploitable vulnerabilities that compromise the security of their LIMS.

### **Layer 3: Network Security**

Most hackers trying to attack internal servers do so remotely through the Internet. They look for vulnerabilities in both the servers and network to gain unauthorized access to LIMS and the valuable data it holds. To protect against such attacks, businesses must ensure that they have properly installed and configured firewalls, Intrusion Detection and Prevention Services, and proactive monitors, to allow only authorized traffic to and from their LIMS servers. Hackers may also use network sniffers to capture data as it is being transmitted from one computer to another – any data that is transmitted over a non-secure connection is vulnerable to theft.

#### **Layer 4: Client Security**

While source data resides on LIMS servers, lab users access their LIMS through desktop and mobile clients. Providing secure access for these clients to the LIMS server, both from within and outside of the lab, is required in order to maintain strong security.

#### **Layer 5: Antivirus**

In addition to trying to obtain content contained within LIMS databases, hackers often send viruses and malware they hope will get installed on corporate desktops and/or servers. From there, these programs can find and send sensitive information back to the hacker or allow the hacker to take control of a computer for use in other attacks.

#### **Layer 6: Administration and Policy Security**

One of the biggest security gaps in corporate systems is actually an internal threat, not external. Specifically, businesses are frequently victims of unauthorized access by employees or consultants who are authorized to administer the LIMS servers. These employees abuse their administrative privileges to access sensitive LIMS information.

#### **Layer 7: Backup and Recovery**

LIMS security goes beyond protection from theft and unauthorized access to also include recovery of data in the case of LIMS server hardware or software failure. Once implemented, a LIMS becomes an integral part of a lab operation; however, few small and medium sized organizations perform regularly scheduled backups of their LIMS systems for quick restoration in the event of a failure. Backup systems and storage media are expensive, and often small and medium organizations do not have the resources required to perform regularly scheduled backups, leaving their workers, and their entire scientific business, exposed in the case of catastrophic hardware or software failure.

---

## **The 10 Layers of Security for Sciformatix SaaS-Hosted LIMS**

Sciformatix treats security as one of its top priorities and works tirelessly to create and maintain the most secure infrastructure possible for its customers. The Sciformatix philosophy is that security is not a one-time problem to fix; it requires ongoing dedication and attention and must be considered in everything the company does. To support this philosophy, Sciformatix designs all of its solutions with strong security considerations and has dedicated security resources whose responsibility is to

secure and monitor the Sciformatix SaaS-hosted LIMS environment. Sciformatix security provisions rival those of world-class enterprises. The 10 layers within the Sciformatix SaaS-hosted model are specified below.

#### **Layer 1: Physical Security**

Sciformatix LIMS applications and data are hosted within a first class state-of-the-art data center that offers the highest levels of security. All areas of the data center are monitored and recorded using cameras, and all access points are controlled with a combined use of biometrics, card readers, alarms, and traditional security measures such as locks and keys. The facility is staffed around-the-clock with security officers and authorized data center personnel who have been authorized with a further layer of security. This system ensures that no unauthorized people can gain physical access to the servers and the overall infrastructure.

#### **Layer 2: Server Security**

Servers are proactively monitored and managed to ensure they are always properly secured. An experienced team of administrators knows how to properly configure each server for maximum performance, without compromising security through open ports or misconfigured user and administrative permissions. Server software is patched with the latest updates and fixes on a regular basis, and antivirus scans are performed regularly to ensure that no malicious software can access customer data. These practices, combined with constant monitoring of the server environments, ensure that the servers hosting and managing your LIMS are always as secure as possible.

#### **Layer 3: Network Security**

The Sciformatix network infrastructure is well protected by a battery of fault-tolerant, brand name firewalls. Each firewall is configured to block unauthorized traffic from entering the network. The Sciformatix policy of redundancy and fault-tolerance ensures that backup systems are immediately up and running if any one firewall fails. In addition to blocking unauthorized traffic using firewalls, Intrusion Detection and Prevention software is used to monitor the traffic flowing into the network, isolate suspicious traffic, and notify the network management and security team of any potential danger.

#### **Layer 4: Client Security**

Sciformatix uses secure sockets layer (SSL) connections to encrypt data sent between the LIMS servers and client workstations. This secure connection protects any data that travels between the LIMS clients and LIMS servers, regardless of whether the client is in the office, home, or using a wireless or public Internet connection at a café or in the airport. Even network sniffers are unable to decipher the data transmitted over the secure connections.

#### **Layer 5: Antivirus**

Sciformatix includes antivirus filtering and protection on all servers, with monitoring and updating taking place on a continuous basis. This solution mitigates the risks of viruses, malware and other attacks on the servers and customers' LIMS data.

### **Layer 6: Administration Policy and Security**

Sciformatix environments are architected so that only authorized accounts can access LIMS services and data, and privileges are assigned to ensure the lowest possible level of access is granted to authorized accounts. Customer accounts can only be assigned access privileges within a home organization and, thus, can only access authorized data for that organization.

### **Layer 7: Backup, Recovery, Mirroring and Automatic Failover**

Regular backups are performed on all database servers, in case data recovery is needed. In addition, with database mirroring, Sciformatix applications and databases will always be available on operational servers, even in the event of catastrophic server failure.

### **Layer 8: Data Obfuscation & Encryption**

In normal in-house implementations, if someone gains access to database files, that data is vulnerable to espionage, theft, or malicious alterations. Beyond physical data security measures, Sciformatix takes the extra precaution of obfuscating LIMS data and can allow for data encryption, providing far stronger data security than typical in-house implementations.

### **Layer 9: Virtual Private Database & Private Database**

Sciformatix uniquely supports two forms of database privacy. The standard virtual private database utilizes multi-tenancy while providing a clean separation of each customer's data. An optional private database scenario provides a customer with completely separate database server instance.

### **Layer 10: Security Validation**

While the security measures above are thorough, it is important to measure that they are indeed providing adequate security for Sciformatix customers. To measure effectiveness of its security infrastructure, tests are performed on a periodic basis, relying on third parties for validation where necessary.

---

## **Conclusion**

A LIMS can be a powerful platform in helping a lab to track its lab information and manage lab processes. But, with the benefits of a LIMS come serious inherent security risks that require ongoing attention. A comprehensive security strategy employs multiple layers of defense from the physical to the digital, and up through the process and policy layers of a LIMS solution. Employing this comprehensive strategy is costly and time-consuming as both an initial investment and on an ongoing basis. Sciformatix is a thought leader on LIMS security and offers one of the most comprehensive and effective security programs for SaaS-hosted LIMS, all included in the low monthly cost of its LIMS offerings.

To learn more about Sciformatix LIMS solutions, please visit [www.Sciformatix.com](http://www.Sciformatix.com).

## About Sciformatix

Sciformatix is a pioneer in providing SaaS-hosted LIMS to scientific labs. The company's breakthrough products include SciLIMS Samples & Storage Management, a Laboratory Information Management System aimed at small-to-medium sized laboratories. Sciformatix solutions allow customers to implement the solution in their lab operations immediately and the solutions put control into the hands of lab professionals, where it belongs. Learn more at [www.sciformatix.com](http://www.sciformatix.com).

