TECHNICAL NOTE

Clarity LIMS™ security, privacy, and compliance

The features and approach that help protect your data

illumina®

Driving strong security and privacy practices

Protecting the privacy of protected health information (PHI), including genomic data, is fundamental to the global business operations of Illumina. Our approach to data protection and privacy, as articulated in our Corporate Privacy Policy, aligns with key standards set by national and global data privacy regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA). We are committed to the following guiding principles:

- Transparency—We clearly communicate our privacy practices and how we use personal data
- Responsible stewardship—We protect personal data to keep it confidential and secure
- Ethical use—We only collect and use personal data in a lawful and transparent manner for purposes that further our mission to improve human health by unlocking the power of the genome
- Accountability—We are committed to complying with all legal requirements and to promoting internal practices to achieve the highest standards for personal data privacy

Security frameworks

Strong institutional privacy practices rely on a successful information security program. While there are various security frameworks in place globally, our practices and this technical note focus on the most common frameworks, including:

- HIPAA
- International Organization for Standardization (ISO) 27001 (security) and 27701 (privacy)

Infrastructure

Illumina applies its own security controls and procedures for Clarity LIMS (laboratory information management system) security along with a comprehensive and well-tested approach inherited from Amazon Web Services (AWS) (Figure 1).[1]

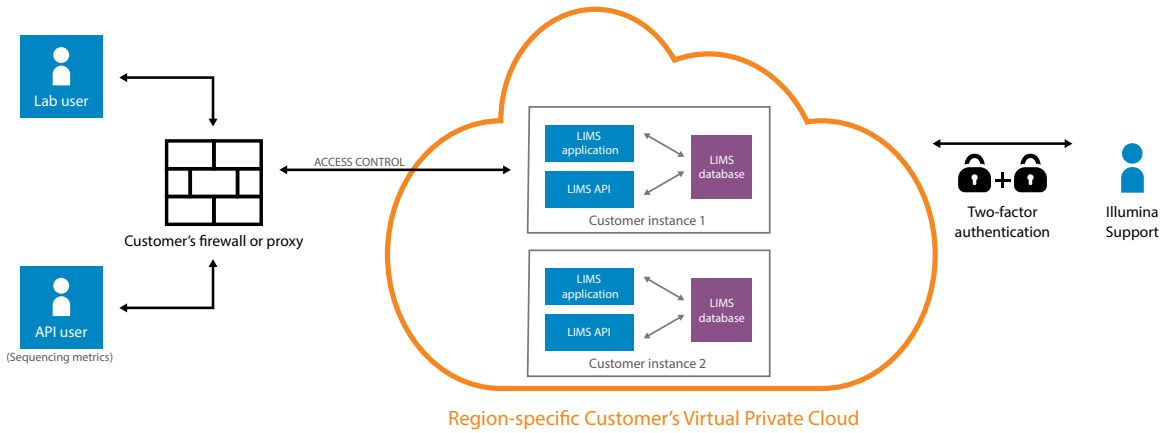

Figure 1: The security infrastructure of Clarity LIMS software.

Security at a glance

A high-level overview of the security controls embodied in Clarity LIMS software is provided in Table 1. Detailed information is provided in the remainder of this technical note.

Table 1: Clarity LIMS security and privacy checklist

Internal and procedural			
Employee background checks	✓	Monitoring	✓
Security policies	✓	Incident response	✓
Access control	✓	Anti-malware	✓
Read-only access assignable to role	✓	Disaster recovery plans	✓
Backups	✓		
Cloud application			
Access control	✓	Anti-malware	✓
Encryption at rest	✓	Disaster recovery	✓
Encryption in transit	✓	Data backup	✓
Logging of activity	✓	Data integrity	✓
Third-party penetration test	✓	Code review/test	✓
Role-based access control	✓	Network	✓
Password controls	✓	Network segmentation	✓
Session management	✓		
Compliance and attestation - Version 5.4 and higher			
ISO/IEC 27001:2022 (for cloud instances)	✓	HIPAA (third-party validated)	✓
ISO/IEC 27701:2019 (for cloud instances, v6.1 and higher)	✓		

Employee security practices

Our security practices start before new employees come onboard. We perform background checks on all employee candidates where permitted by law. Documented policies guide personnel in preventing, detecting, and containing any security violations.

A security awareness and training program communicates security policies to employees who develop or support Clarity LIMS software. An automated training system makes sure that all required employees complete this training.

All employees who support Clarity LIMS software are required to undergo annual training regarding how to handle customer data. Access to customer systems is granted on a per-employee basis. Downloading of data is restricted, and all activity is logged and documented. When employees who supported Clarity LIMS software leave the company, their access to all customer systems and internal Illumina systems is revoked. All equipment and badges supplied to the employee are relinquished.

Information management system

ISO/IEC 27001:2022 and ISO/IEC 27701:2019 for Clarity LIMS cloud

ISO 27001:2022 is an information security management system (ISMS) that seeks to place all information security management under the governance of management, ensuring that processes and policies are consistently and reliably deployed and enforced. The standard dictates how data are stored and managed and how information assets are disposed. ISO/IEC 27701:2019 is a privacy information management system (PIMS) standard that certifies robust data privacy requirements are implemented to ensure data are stored and maintained in a private and compliant manner. The policies in place for ISO/IEC 27001:2022 and ISO/IEC 27701:2019 also establish standards for access control, password management, and network security.

Illumina ISO certification

HIPAA

Our facilities where PHI is processed are in compliance with HIPAA and industry best practices. Examples of the best practices we follow:

- Buildings are monitored 24 hours a day and keycard accessed
- Offices have a monitored security system
- Computers used to access or store PHI are password protected and have full-disk encryption turned on
- Any access from outside the office is via a secure Virtual Private Network (VPN)

Clarity LIMS development

Clarity LIMS software is developed and tested to create a sound, usable, and predictable experience for users. The software development process determines prioritization of features, functionality, and bug fixes based on business needs and customer input. We use an Agile methodology to develop Clarity LIMS software. The particular implementation of the Agile manifesto is Scrum, which is a widely used and accepted method of running the development process.

The major features of Agile include short development cycles called sprints, the ability to change and adapt to marketing and technical needs, and constant review and improvement of the process. After completion, all code changes are reviewed by at least two other developers, except in the case of small wording changes. The review process helps developers identify issues in the code base, or use of code patterns that are not up to standards. Code that is not up to standards will be revised and reviewed until it meets standards. The Agile methodology allows for multiple checkpoints designed to deliver a system that meets or exceeds customer expectations. This and other quality assurance measures, such as automated code checking, make sure delivered systems are fit for their given purpose and that the processes used are correct and suitable.

Implementation and updates of Clarity LIMS cloud

From time to time, Illumina will release security and operating system (OS) patches, bug fixes, and other releases. When security and Clarity LIMS patch versions are released, Illumina will update the applicable Clarity LIMS instances during regularly scheduled windows. As part of our patching activities, the following may be upgraded:

- Underlying OS patches
- Underlying included software or Clarity LIMS patches
- Illumina tooling, including antivirus, logging, intrusion detection, backups, etc
- Additional components of the system that do not break standard Clarity LIMS functionality for the deployed version

For minor and major releases, Illumina personnel will coordinate upgrade timing with customers and provide end of life, hosting, and support notifications for older versions. Illumina will typically apply patch versions to all applicable hosted versions during regularly scheduled windows, unless security or other requirements require more rapid response. After the announced End of Support (EOS) date, Illumina may upgrade older versions to the newest Clarity LIMS release.

Security practices in Clarity LIMS software

Clarity LIMS software includes several features and measures to promote safety and privacy of PHI data.

Access control

Laboratory work requires staff with a diverse set of skills who work on a wide array of tasks. To prevent error, data loss, or tampering, system access is restricted based on which roles require access. Clarity LIMS software includes configurable access control, with the ability to assign read-only access via role-based permission settings (enabled as of Clarity LIMS v6.1).

Users with admin roles can configure access such that designated users have read but not write access. Read-only mode supports secure data access for a range of customer use cases, including auditing, reporting, and training.

Encryption at rest (cloud application)

When data are at rest, Clarity LIMS software uses Advanced Encryption System (AES)-256 to protect data. AES-256 is a well-known encryption system that is easy for developers to use but difficult for hackers to crack because of its lengthy 256-character key. AES-256 is reliably used in financial, government, and health care industries throughout the world.

Encryption in transit

To protect data in transit, Clarity LIMS software uses Transport Layer Security (TLS) 1.2 or newer. TLS is a standard and well-established technology for encrypting the link between a web server and a web browser. Like Advanced Encryption Standard (AES)-256, TLS is reliably used in many industries, including health care.

Activity logging

In any lab, sample traceability is important, but it becomes even more important when working in compliance-driven environments. Clarity LIMS software supports compliance by producing an audit trail of any sample in the system.

An audit trail is a detailed account of the sample and every action taken on the sample since its creation in the LIMS. Labs can use the audit trail produced in Clarity LIMS software to inform system reporting or to satisfy audit requirements. The audit trail in Clarity LIMS software details all events in the lifetime of a sample:

- Date and time of sample acquisition and upload
- Lab users responsible for any actions taken on the sample
- Reagents used with the sample

Authentication

Clarity LIMS software uses a single-factor authentication process. Users log on via a web portal using their credentials. Organizations can integrate their corporate passwords process such that Clarity LIMS users can log on using their corporate passwords and Lightweight Directory Access Protocol (LDAP) process. Integrating with LDAP is available as part of Clarity LIMS Enterprise software.

With Clarity LIMS v6.3 and higher, users have the option to integrate with the Illumina Platform Auth Service (PAS). This Single-Sign-On (SSO) authentication method allows customers already logged into PAS to access Clarity LIMS without needing to log in again.

Session management

Clarity LIMS software includes a session management feature to log out users automatically after 30 minutes of inactivity. Session management can be configured by users with admin privileges.

Prevention of network and application vulnerabilities

Boundary controls monitor and regulate communications, the external boundary of the network, and key internal boundaries. These boundary controls employ rule sets, access control lists, and configurations to enforce the flow of information to specific information system services. Access control lists, or traffic flow policies, are established on each managed interface to regulate the flow of traffic. Additional controls include:

- Periodic network scanning
- Policy against use of email for data delivery, mitigating risk from attachments that could contain malware
- Prioritized response for critical security issues

Third-party penetration testing

Third-party penetration tests simulate an attack on a system's deployment and are a good way to test defenses actively. Illumina employs an unbiased third party to conduct pen tests for Clarity LIMS cloud instances. After the vendor finishes the test, Illumina receives a comprehensive report, detailing the results. Illumina does not release the results of these penetration tests.

Data integrity*

Customer database backup occurs up to 24 times per day to decrease the risk of data loss. In addition, the system contains logging that provides notification when data are altered. If improper alteration is detected, rolling back to a previous backed up version is available.

Data backups

Clarity LIMS cloud undergoes a rigorous backup process to protect against data loss or disaster. Data are backed up using an automated system. Both the database and associated external data files and appropriate system configuration are backed up. Backups are encrypted in transit to an S3 storage area accessible by authorized staff only. Illumina retains three sets of backups from the time that they are created:

- Backups every four hours retained for two days
- Daily backups retained for 32 days
- Monthly backups retained for 400 days

Disaster recovery

In the event of a disaster, a new cloud system will be created and configured and a backup will be restored. After the new system is implemented, Illumina will work with system users to test and make sure that all data are in place.

We plan a disaster recovery test annually. As new versions of the software are released, it is possible that the backup and disaster recovery plan will need to change. Any necessary changes will be made to the backup and recovery system before going live with any customer data.

Support for HIPAA

Clarity LIMS software is designed and implemented to support HIPAA. The United States Congress enacted HIPAA in 1996, and thereafter, the United States Department of Health and Human Services implemented multiple regulations to carry out the law in practice.[2] Among other things, HIPAA established national standards for the security and privacy of PHI. Major provisions for HIPAA include the Security Rule and Breach Notification Rule.

The HIPAA Security Rule establishes several requirements to ensure the security and privacy of PHI. Clarity LIMS software includes, but is not limited to, security control requirements (Table 1, Table 2).

GDPR

GDPR does not only apply to companies established in the EU. Companies established outside of the EU, but targeting individuals in the EU, may also be subject to the GDPR.

As data controllers, customers are ultimately responsible for assessing the applicability of the GDPR to their processing operations and ensuring that they have a GDPR-compliant practice in place. However, given that the GDPR is relevant to many of our customers, Clarity LIMS follows GDPR principles applicable to data processors.

Shared responsibilities

Illumina is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Part of this responsibility requires that Illumina perform recurring security patch updates or other updates to protect the environment from emerging threats and support iterative improvements. Illumina provides these updates during weekly windows defined in the Clarity LIMS software Terms and Conditions. Customers required to comply with HIPAA are responsible for ensuring they have a HIPAA compliance program in place and the appropriate Clarity LIMS subscription with a signed BAA.

Security controls

Using Clarity LIMS software places several responsibilities in the hands of the customer. Risk assessment must account for the use of software as a service (SaaS) solutions, and outcomes of these assessments should be reflected in a review of privacy and security controls of each customer. Customers should review their policies to

* Data integrity, data backup, and disaster recovery mitigations are performed for Clarity LIMS cloud software only.

reflect the use of Clarity LIMS software. Institutions should establish processes and procedures for access approval and implement regular reviews of access that has been granted to all users. Furthermore, workstations used to access Clarity LIMS software must have proper protections installed, such as antivirus software, host-based firewalls, and centralized logging. Business continuity and disaster recovery plans should be updated to account for the use of Clarity LIMS software.

Table 2: Security controls in Clarity LIMS software

Administrative controls
Policies and procedures to prevent, detect, contain, and correct security violations
Security official responsible for developing and implementing controls within the organization
Procedures to make sure that workforce members access to data is appropriate and approved
Read-only access permission setting
Processes to authorize access to customer data
Workforce members trained on HIPAA
Processes for incident reporting
Routine evaluation to determine how changes to other procedures or the environment can potentially impact security
Physical controls
Implemented facility access controls
Clarity LIMS software hosted in secure data centers
Policies regarding workstation security
Technical controls
Unique user ID for each user
User authentication by Clarity LIMS software or a customer's LDAP
Encryption of data in transit and at rest

Incident response and breach notification

Under HIPAA, Business Associates are required to comply with a set of rules and regulations regarding potential and actual breaches. If there has been an attempted breach, Illumina will complete a risk assessment to determine if the attempt constitutes an actual breach. If so, Illumina will notify the customer as soon as reasonably possible, provided that unsuccessful attempts, such as pings and other broadcast attacks on our firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, do not constitute an attempted breach.

Laboratory compliance

Clarity LIMS software includes numerous features to support compliance with regulations, standards, and accreditations applicable to laboratories running tests on human samples, such as CLIA, CAP, and ISO 15189. These include:

- Sample tracking and complete sample histories for audit purposes
- Tools that help comply with standard operating procedures
- Reagent and lot tracking
- Role-based interfaces that enable access only to authorized functions
- Security features, as described in this technical note

Learn more

Clarity LIMS software

References

1. Amazon Web Services. AWS Cloud Security. aws.amazon.com/security/. Accessed July 18, 2024.
2. US Department of Health & Human Services. Summary of the HIPAA Privacy Rule. hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Updated October 19, 2022. Accessed July 18, 2024.
3. Centers for Medicare & Medicaid Services. cms.gov/. Accessed July 18, 2024.
4. Centers for Medicare & Medicaid Services. CLIA Regulations and Federal Register Documents. cms.gov/Regulations-and-Guidance/Legislation/CLIA/CLIA_Regulations_and_Federal_Register_Documents. Updated December 1, 2021. Accessed July 18, 2024.
5. College of American Pathologists. Accreditation. cap.org/laboratory-improvement/accreditation. Accessed July 18, 2024.

illumina®

1.800.809.4566 toll-free (US) | +1.858.202.4566 tel
techsupport@illumina.com | www.illumina.com

M-GL-00704 v4.0