

BaseSpace™ Clarity LIMS security and privacy

Learn about the features and approach that help protect genomic data.

Introduction

To store and manage the growing body of genomic data generated, many researchers are turning to cloud computing environments. Undeniably, cloud computing can offer genomics researchers many benefits including low IT overhead, scalable storage and computing, and ease of access. However, many who operate and work in life sciences labs are skeptical about how safely data, especially protected health information (PHI), can be stored and managed.

So that customers can benefit from the cloud while keeping PHI secure, Illumina has developed a robust set of security and privacy practices to govern the way our informatics software is created, deployed, and used in the cloud. BaseSpace Clarity LIMS (Laboratory Information Management System) is informatics software that helps labs gain efficiencies and throughput with increased accuracy, fast turnaround, sample traceability, and ready-to-use instrument integrations.

BaseSpace Clarity LIMS cloud version is a software-as-a-service (SaaS) offering for genomics laboratory information management, placing high priority on protecting the confidentiality, integrity, and availability of customer data. This technical note describes the set of comprehensive policies, processes, and controls enacted for security and privacy.

Security and compliance frameworks

While there are several security and compliance frameworks in place globally, our practices and this technical note focus on the most common frameworks, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- International Organization for Standardization (ISO) 27001
- Service Organization Control (SOC)
- Clinical Laboratory Improvement Amendments (CLIA)
- College of American Pathologists (CAP)

Infrastructure

Illumina applies its own security controls and procedures for BaseSpace Clarity LIMS security along with the comprehensive and well-tested approach of Amazon Web Services (AWS) (Figure 1).¹

Security and privacy at a glance

A high-level overview of the privacy and security measures embodied in BaseSpace Clarity LIMS is provided (Table 1). For more detailed information, see the remainder of this technical note.

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 BaseSpace Clarity LIMS. An automated training system makes sure that all required employees complete this training. Furthermore, all employees who support BaseSpace Clarity LIMS are subject to disciplinary action for failure to comply with the stated security policies.

All employees who support BaseSpace Clarity LIMS are required to undergo annual training regarding how to handle customer data. Employees are granted access to customer systems for support on an as-needed basis. Downloading of data is restricted, and all activity is logged and documented in an automated system. If employees who supported BaseSpace Clarity LIMS leave the company, then their access to all customer systems and Illumina-internal systems are revoked. All equipment and badges supplied to the employee are also relinquished.

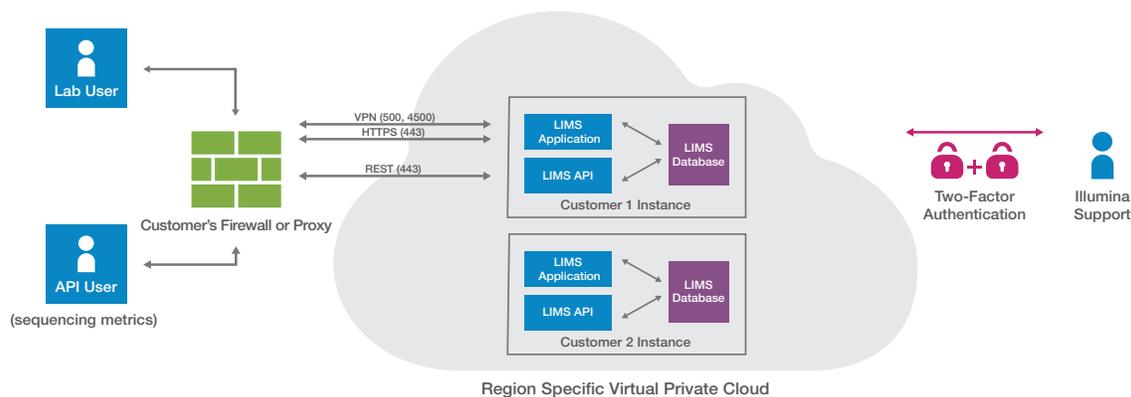


Figure 1: The security infrastructure of BaseSpace Clarity LIMS

Table 1: BaseSpace Clarity LIMS security and privacy checklist

Internal and procedural			
Employee background checks	X	Monitoring	X
Security policies	X	Incident response	X
Access control	X	Anti-malware	X
Application			
Access control	X	Disaster recovery	X
Encryption at rest	X	Data backup	X
Logging of activity	X	Data integrity	X
Third-party pen test	X	Code review/test	X
Multi-factor authentication		Network	X
Role-based access control	X	Encryption in transit	X
Password controls	X	Encryption at rest	X
Session management	X	Network segmentation	X
Anti-malware	X		
Facility			
ISO 27001		Compliance	
SOC	X	HIPAA	X
HIPAA (US)	X	AT 101 audit	
Secure facilities	X	Will sign business associate agreement with Amazon Web Services	X
Backups	X	European union data	X ^a
Disaster recovery plans	X		

a. For Germany and Ireland

Facility-related measures

Several information security management systems are in place at our facilities to provide an efficient and secure workplace for employees and information assets.

ISO 27001:2013

ISO 27001:2013 is an information management security standard that seeks to place all information security management under the governance of management, so that processes and policies are consistently and reliably deployed and enforced. The standard dictates how data are stored, managed, and how information assets are disposed of. The policies in place for ISO 27001:2013 also establish clear standards for access control, password management, and network security. Illumina follows guidelines in accordance with ISO 27001:2013, and the location in which BaseSpace Clarity LIMS is developed is in the process of being audited.

HIPAA

Our facilities are in compliance with HIPAA and general best practices:

- Our buildings are monitored 24 hours a day. Building is key-card accessed from both the front door of the building and the front door of our office.
- Our 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).

Development of BaseSpace Clarity LIMS cloud

The software is developed and tested to create a sound, usable, and predictable experience for users. The software development process for BaseSpace Clarity LIMS determines prioritization of features and functionality and bug fixes based on business needs and customer input. We use an Agile methodology to develop BaseSpace Clarity LIMS. 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 tiny 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 to ensure the system delivered meets or exceeds customer expectations. The quality assurance measures in place help to make sure that systems delivered are fit for their given purpose, and that the processes used are correct and suitable.

Implementation and updates of BaseSpace Clarity LIMS cloud

From time to time, Illumina will release bug fix patches to BaseSpace Clarity LIMS customers. When upgrades are released, Illumina will schedule them during a short upgrade window with as much notice as possible shortly after the patch is released. Note that as a part of major software releases, the following may also be upgraded:

- Underlying operating system version
- Underlying database technology version
- Proxy software or related components version
- Illumina-specific tooling version (anti-virus, logging, intrusion detection, backups)

Security practices in BaseSpace Clarity LIMS

BaseSpace Clarity LIMS 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, regulations such as 21 CFR Part 11 require that system access be restricted based on which roles require access and the system tasks those roles are required to complete. For instance, technicians responsible for quality control or sample accessioning only should not have access to system functionality for completing a sequencing run or analysis results. BaseSpace Clarity LIMS includes configurable access control. Users with the proper permissions can configure access such that only those who are required see certain areas of the application.

As for access of customer data to internal staff, access is granted on an as-needed basis only. If the customer database is needed to reproduce an issue, development will write a script to remove any sensitive data before using the database for internal testing to avoid any possible breach in security.

Encryption at rest

When data are at rest, BaseSpace Clarity LIMS 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 healthcare industries throughout the world.

Encryption in transit

To protect data in transit, BaseSpace Clarity LIMS uses Transport Layer Security (TLS). TLS is a standard and well-established technology for encrypting the link between a web server and a web browser. Like AES-256, TLS is reliably used in many industries, including healthcare.

Activity logging

In any lab, sample traceability is important, but it becomes even more important when working in compliance-driven environments. BaseSpace Clarity LIMS 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 BaseSpace Clarity LIMS to inform system reporting or to satisfy audit requirements. The audit trail in BaseSpace Clarity LIMS 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

BaseSpace Clarity LIMS 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 BaseSpace Clarity LIMS users can log onto the system using their corporate passwords and LDAP process. Integrating with LDAP is available as part of BaseSpace Clarity LIMS Enterprise.

Session management

BaseSpace Clarity LIMS includes a session management feature to automatically lock after 30 minutes of inactivity. This feature is configurable by users with admin privileges.

Prevention of network and application vulnerabilities

Boundary controls monitor and regulate communications and the external boundary of the network, and at 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 validation (pen test)

Third-party pen (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 penetration tests annually or as substantial change warrants. After the vendor finishes the test, Illumina receives a comprehensive report, detailing the results. The test includes information about the test, how far the tester was able to breach, if at all, our defenses, and suggestions for mitigating any issues.

Data integrity

Customer databases are backed up 24 times per day, thereby decreasing the risk of data loss. In addition, the system contains logging that notifies us when data are altered. If improper alteration is detected, we can roll back to a previous backed up version.

Data backups

BaseSpace 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 stored in an S3 storage area only accessible by authorized staff only. Illumina retains three sets of backups:

- Hourly backups are retained for two days after they are created
- Daily backups are retained for one month after they are created
- Monthly backups are retained for 13 months after they are created

Disaster recovery

In the event of a disaster, a new hosted system will be installed and configured and the data backup will be put into place. After the new system is implemented, Illumina will work with the users of the system to test to make sure 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.

HIPAA Compliance

BaseSpace Clarity LIMS was designed and implemented to support HIPAA-compliance. 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. BaseSpace Clarity LIMS includes but is not limited to controls requirements (Table 1, Table 2).

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 that responsibility requires that Illumina perform

Table 2: Security controls in BaseSpace Clarity LIMS

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 date are appropriate and approved
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
BaseSpace Clarity LIMS hosted in secure data centers
Policies regarding workstation security
Technical controls
Unique user ID for each user
User authentication by BaseSpace Clarity LIMS or a customer's own authentication system
Encryption of data in transit and at rest

recurring security patch updates or other controls implementation to protect the environment from emerging threats and support iterative improvements. It is the Customer's responsibility to coordinate/permit Illumina to update Clarity LIMS on a recurring basis. Customers required to comply with HIPAA are responsible for ensuring that they have a HIPAA compliance program in place and that they use BaseSpace Clarity LIMS in a manner to ensure their compliance.

Illumina will execute a Business Associate Agreement (BAA) with BaseSpace Clarity LIMS customers upon request. A BAA is a contract between a HIPAA entity and a business associate. The contract protects personal health information and stipulates how it will be handled. Illumina also has a BAA with Amazon Web Services for BaseSpace Clarity LIMS.

Security controls

Using BaseSpace Clarity LIMS places several responsibilities in the hands of the customer. Risk assessment must account for the use of 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 reflect the use of BaseSpace Clarity LIMS. For example, password policies should prohibit the sharing of BaseSpace Sequence Hub accounts and passwords. Institutions should establish processes and procedures for the approval of access and implement regular reviews of access that has been granted to all users. Furthermore, workstations used to access BaseSpace Clarity LIMS 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 BaseSpace Clarity LIMS.

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. The notification will include the following:

- A brief description of what happened, the date on which it happened, and the date on which the breach was discovered
- The names of all individuals who have been affected by the breach
- A description of the types of data included in the breach
- Recommended steps that individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of what the Business Associate is doing to investigate the breach and as to prevent further breaches. BaseSpace Clarity LIMS customers are responsible for contacting their customers in the event of a breach.

CLIA and CAP compliance

Many Illumina customers sequence human samples. Such laboratories are under the authority of the Centers for Medicare and Medicaid Services (CMS)³, as described by the Clinical Laboratory Improvement Amendments of 1988 (CLIA Regulations).³ The CLIA regulations establish quality standards for laboratory testing performed on human specimens for diagnosis, prevention, treatment of disease, or assessment of health. CLIA regulations are designed to ensure the accuracy, reliability, and timeliness of test results. Regulations include quality standards for proficiency testing, test management, quality control, personal qualifications, and quality assurance. Clinical labs can choose to be evaluated under more rigorous standards set by the College of American Pathologists⁵. From a regulatory perspective, CAP standards have been recognized as above and beyond what is required by CLIA. Therefore, CMS deems CAP accreditation compliant with CLIA regulations.

Although users of BaseSpace Clarity LIMS are not required to achieve compliance in all situations, the system includes numerous features to support it. These include:

- Sample tracking and complete sample histories for audit purposes
- Tools that help comply to standard operating procedures
- Reagent and lot tracking
- Role-based interfaces that enable access only to authorized areas
- Security features, as described in this technical note
- Precision monitoring via a Run Summary report that helps labs validate that instruments are running according to specification
- System validation— Illumina offers system validation for labs that don't have the resources to complete the validation

References

1. Amazon Web Services. Accessed March 2020.
2. [Summary of the HIPAA Privacy Rule](#). Accessed March 2020.
3. [Centers for Medicare & Medicaid Services](#). Accessed March 2020.
4. [College of American Pathologists](#). Accessed March 2020.