SECURITY BRIEF

BaseSpace™ Sequence Hub security and privacy

Protecting genomic data in a secure cloud environment

illumina®

BaseSpace Sequence Hub

BaseSpace Sequence Hub is an easy-to-use, cloud-based genomics run management, bioinformatic analysis, and secure data storage environment. This white paper describes the comprehensive processes, controls, and features of BaseSpace Sequence Hub that support the security, privacy, and compliance requirements of lab sequencing operations.

Software development lifecycle

BaseSpace Sequence Hub is implemented as a single instance, multitenant deployment. Updates are transparent, requiring no user action. All major upgrades are communicated via release notes at least two weeks in advance.

Business needs and customer input determine the prioritization of the software development life cycle (SDLC) of BaseSpace Sequence Hub features, content, functionality, and bug remediation. Software is engineered and unit-tested using contemporary agile development methodologies. Service updates are relatively small and frequent, reducing the risk of customer impact. Validation of changes in BaseSpace Sequence Hub involves automated regressions and manual testing and occurs in a test environment that is segregated from a staging/production environment.

To address platform security, the well-tested approach of Amazon Web Services (AWS)[1] is combined with internal testing procedures. Together, these methods provide a cloud-based genomics solution that meets the security needs of institutional IT infrastructures. This white paper describes the security features of BaseSpace Sequence Hub, which supports customer compliance with various regulations and standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US, and the General Data Protection Regulation (GDPR) in the European Union (EU).

Security practices in BaseSpace Sequence Hub

BaseSpace Sequence Hub imports data directly from the sequencing instrument during the run, enabling customers to begin data analysis immediately after the run is completed. Several security measures protect data in transit during communication between the sequencing instrument and the data analysis (Table 1).

Users can store data both locally and in BaseSpace Sequence Hub in the cloud. Illumina sequencing platforms (MiniSeq™, MiSeq™, NextSeq™, HiSeq™, and NovaSeq™ Systems) support encryption in transit and verification of data generated during a run. The brokering software interacts with the application program interface (API), allowing network interruptions, latencies, and incomplete transmissions to be caught and requeued automatically. During run setup, the user initiates the decision to send data to BaseSpace Sequence Hub. If this option is chosen, the run is authenticated against, and tracked to, a user account. For large organizations with multiple users, BaseSpace Sequence Hub Enterprise provides single sign-on access with third-party authentication that uses standards of security assertion markup language (SAML) 2.0 controlled access.

Users are required to remove all direct personal identifiers (eg, names, dates of birth) from samples that they upload to BaseSpace Sequence Hub.[2] Sample tracking is accomplished by providing unique codes, such as bar codes or random sample identifiers, to each sample before uploading. BaseSpace Sequence Hub customers should store any direct identifier information in a separate encrypted system outside of BaseSpace Sequence Hub.

Global standards and certifications

BaseSpace Sequence Hub is International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001:2013 and 27701:2019 certified by an independent auditor for the full scope of its activities, including development, management, and support of a cloud-based analysis platform. ISO 27001:2013 is an information security standard that seeks to place all information security management

Table 1: Security controls in BaseSpace Sequence Hub

Security control	Description
Administrative	• Policies and procedures to prevent, detect, contain, and correct security violations • Security official responsible for developing and implementing security policies and controls • Procedures to make sure that workforce member access to customer data is appropriate and approved • Processes to authorize access to customer data • Workforce members trained for security policies • Processes for incident reporting • Periodic evaluation of environmental and operational changes that impact the security of the data • Privacy Impact Assessments (PIAs) performed for all new features that handle user data
Physical	• Implemented facility access controls • BaseSpace Sequence Hub hosted in secure data centers • Policies regarding instrument control computer security • Policies and procedures for mobile devices • Maintained inventory of devices supporting BaseSpace Sequence Hub
Technical	• Unique user ID for each user • User authentication by BaseSpace Sequence Hub or the identity management system of the customer organization • Protection of integrity of data in transit • Transport Layer Security–based encryption in transit (version 1.2 or newer) • User-initiated data deletion capability
ISO 27701	• Information security policies • Organization of information security • Access control • Encryption • Physical, environmental, and operational security • Information security incident management • Information security aspects of business continuity management

under a set of clearly described principles, 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 standard that certifies how 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 27001:2013 and ISO/IEC 27701:2019 also establish standards for access control, password management, and network security.

BaseSpace Sequence Hub was developed in accordance with the Illumina SDLC process under the Illumina Quality Management System (QMS). Additionally, processes within the Illumina QMS have adopted industry best practices and relevant standards, including:

- ISO/IEC 27001:2013
- ISO/IEC 27701:2019
- ISO 13485
- HIPAA (third-party validated)

Security in transit

BaseSpace Sequence Hub communicates with instruments through a web-based API. All traffic between the sequencing instrument and BaseSpace Sequence Hub uses Transport Layer Security (TLS) version 1.2 or newer, an internet standard that encrypts sensitive communications as they pass over the internet. All service methods require API key signatures, and service is refused to all others. Requests are monitored for abuse.

Access to BaseSpace Sequence Hub

To access BaseSpace Sequence Hub, users log in via a web portal. Users can be identified with BaseSpace Sequence Hub authentication or using single sign-on for enterprise customers. BaseSpace Sequence Hub

Enterprise customers can dictate policies for password length and complexity and configure account lockout and lockout duration to protect against password brute forcing.

Invalid login attempts and logoffs are recorded by the system. If enterprise customers use a single sign-on, login activity may also be monitored from the customer systems. Changes, reads, updates, deletions, and shares of customer data are also logged for BaseSpace Sequence Hub Enterprise customers. Logs can be monitored for suspicious user activity and are available as *.csv files or via API. All computation instances are run within Virtual Private Clouds, providing a logically isolated section of the AWS cloud, where AWS resources reside in a virtual network defined by Illumina.

Data integrity

Through AWS, BaseSpace Sequence Hub stores customer data synchronously across multiple availability zones, performs regular data integrity checks, and self-heals to protect against data loss. However, BaseSpace Sequence Hub is not an unlimited backup system. There is no mechanism to retrieve deleted data.

Encryption at rest

Customer data in BaseSpace Sequence Hub is encrypted at rest using the AES-256 standard.

Risk analysis and third-party penetration testing

With persistent risk analysis and security testing, we continue to improve the cybersecurity of all our products and practices. Illumina continually assesses the cybersecurity risk environment and the posture of our instrument installation base by working with our industry partners, customers, and support teams. We use our understanding of evolving cybersecurity risks and threats to design new products to a higher standard and implement up-to-date enterprise-wide cybersecurity practices.

Illumina performs continuous security testing of our software code for all cloud software products. As part of our standard build process, software code regularly undergoes static analysis for security defects. External penetration testing experts validate existing Illumina cloud software products on an annual basis. After the vendor finishes the test, Illumina receives a comprehensive report detailing the results. Illumina does not release the results of these penetration tests.

Preventing network and application vulnerabilities

Boundary controls monitor and regulate communications at 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
- System hosts (virtual instances) deployed as known fixed images
- Automated secure code scanning adhering to Open Web Application Security Project (OWASP) guidance*
- Network and host-based security controls

Data sharing by users

BaseSpace Sequence Hub is designed as a collaborative system. Users are responsible for following internal organizational policies for regulating who can share or transfer data. Users share data and grant access rights within the application by sending a request to share to another registered user.

* OWASP is an organization that provides unbiased, practical, and cost-effective information about computer and internet applications.

Users can temporarily share data access with technical support when legally permitted. On occasion, troubleshooting or user training can be done via screen-sharing or remote computing tools such as RescueAssist and TeamViewer.

Data backups

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

- Hourly backups 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.

Data center security

BaseSpace Sequence Hub is built on preexisting cloud infrastructure provided by AWS and, therefore, shares several AWS standards and accreditations (Table 2). More information on AWS security features is available on the Amazon website.[1]

Illumina employee security practices

Background checks are performed on all Illumina employment candidates in the United States. The background check includes education, previous employment, and criminal records. Documented policies and procedures are in place to guide personnel in preventing, detecting, containing, and correlating security violations.

A security awareness and training program communicates Illumina security policies to employees that support BaseSpace Sequence Hub. An automated compliance monitoring system tracks employee compliance with training requirements. All Illumina employees supporting BaseSpace Sequence Hub are aware of disciplinary action for failure to comply with Illumina security policies.

All Illumina employees who support BaseSpace Sequence Hub software are required to undergo annual training regarding proper handling of 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 in an automated system. When employees who have supported BaseSpace Sequence Hub software leave the company, their access to all

Table 2: Amazon Web Services standards and accreditations

Feature	Description
Service Organization Controls 1/Service Organization Controls 2/SSAE 16/ISAE 3402	An audit framework for verifying that AWS controls to protect customer data are properly designed and that the individual controls are operating effectively based on clearly described standards
Federal Information Security Management Act (FISMA) Moderate	An accreditation granted by the US Government to strengthen federal information system security using the Risk Management Framework put forth by the National Institute of Standards and Technology

customer systems and internal Illumina systems is revoked and all equipment and badges supplied to the employee are relinquished.

Privacy by design

Illumina uses a privacy-by-design approach that ensures customers' sensitive data are protected with strong encryption standards and strict controls for data access. BaseSpace Sequence Hub supports customers operating in regulated environments and is in accordance with current data protection laws, including GDPR and HIPAA.

HIPAA

HIPAA Security Rule requirements include administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).[3] BaseSpace Sequence Hub offers several features and controls to support the requirements of the HIPAA Security Rule (Table 1).

Customer responsibilities under HIPAA

Customers required to comply with HIPAA are ultimately responsible for ensuring that they have a HIPAA-compliant program in place and that they use BaseSpace Sequence Hub in a manner that ensures their compliance.

Illumina will execute a Business Associate Agreement with BaseSpace Sequence Hub customers upon request. Illumina has a Business Associate Agreement with AWS for BaseSpace Sequence Hub. Establishing a Business Associate Agreement with Illumina helps support customer HIPAA compliance.

GDPR privacy and compliance

BaseSpace Sequence Hub is designed and built to meet the standards laid out in the GDPR by the EU. This compliance extends to all global instances of BaseSpace Sequence Hub. GDPR applies to companies located in the EU and to non-EU companies targeting individuals in the EU. Because GDPR is relevant to many of our customers, BaseSpace Sequence Hub is designed with included GDPR requirements applicable to use of BaseSpace Sequence Hub as a data processor (Table 1).

Customer responsibilities under the GDPR

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. As data controllers, customers should use BaseSpace Sequence Hub in a manner that ensures compliance with applicable regulations.

Customer-implemented security controls

The use of BaseSpace Sequence Hub puts several responsibilities in the hands of the customer, which aligns with the AWS model of shared responsibility. Customers should perform risk assessments to account for the use of software-as-a-service (SaaS) solutions and outcomes of the risk assessment should be reflected in a review of privacy and security controls for each customer.

Customer policies should be reviewed to reflect the use of SaaS solutions. For example, password policies should prohibit the sharing of BaseSpace Sequence Hub accounts and passwords. Institutions should establish processes and procedures for access approval and implement regular reviews of granted user access. Additionally, customers should review and establish best practices encompassing the content of the data submitted to BaseSpace Sequence Hub. For example, naming policies should prohibit the introduction of identifying subject information.

Instrument control computers used to access BaseSpace Sequence Hub should have proper protections installed, such as antivirus software, host-based firewalls, centralized logging, etc. Business continuity and disaster recovery plans should be updated to account for the use of BaseSpace Sequence Hub.

Breach notification

Where notification thresholds are met, BaseSpace Sequence Hub customers are ultimately responsible for notifying individuals whose data may have been compromised as part of a breach and notifying data protection authorities. An audit trail API will be made available to Enterprise administrators containing information about every instance of attempts to access user data (all file types that are potentially accessible). This includes invalid logon attempts, logoffs, downloads, views, and shares. The log includes date, time, user, and a description of each action. The description of data modification comprises the name of the tool, or the API call, used to modify the data. An API enables users to administer the audit log in an external system.

CLIA and CAP

Many Illumina customers perform sequencing on human samples. Such laboratories are under the authority of the Centers for Medicare and Medicaid Services (CMS)[4] as described by the Clinical Laboratory Improvement Amendments of 1988 (CLIA Regulations).[5] 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, personnel qualifications, and quality assurance. Clinical labs can choose to be evaluated under more rigorous standards set by the College of American Pathologists (CAP).[6] From a regulatory perspective, CAP standards have been recognized as above and beyond what is required by CLIA regulations. Therefore, accreditation by CAP is formally deemed by CMS to certify compliance with CLIA regulations as well.

BaseSpace Sequence Hub support for CLIA and CAP

CLIA and CAP labs can use BaseSpace Sequence Hub to store, manage, and analyze sequencing data. Use of BaseSpace Sequence Hub does not require CLIA and CAP validation because it does not interpret data received from health care providers. BaseSpace Sequence Hub provides several key features that enable labs to ensure data integrity, accuracy, and reliability. The ability to demonstrate reproducibility and to track the origin of analysis results enables customer adherence to CLIA and CAP standards:

- A checksum is performed on all data uploaded directly from the sequencing instrument to ensure integrity with the source data
- All data, including genomic data, in S3 is immutable
- BaseSpace Sequence Hub apps are version-controlled and procedures are in place to prevent modification to published apps
- Functions that can alter the interpretation of a result are versioned and users can continue to use the previous version until a new round of validation is complete
- Detailed logs describe every analysis performed

Learn more

BaseSpace Sequence Hub

References

1. Amazon Web Services. Cloud Computing Serices-Amazon Web Services. aws.amazon.com. Accessed July 12, 2023.
2. Illumina. BaseSpace Sequence Hub User Terms of Use. basespace. basespace.illumina.com/agreements/current/details?category=USER. Accessed July 12, 2023.
3. US Department of Health and Human Services. Health Information Privacy. hhs.gov/hipaa/. Accessed July 12, 2023.
4. Centers for Medicate and Medicaid Services. cms.gov. Accessed July 12, 2023.
5. Centers for Medicate and Medicaid Services. Clinical Laboratory Improvement Amendments (CLIA). cms.gov/Regulations-and-Guidance/Legislation/CLIA/index.html. Accessed July 12, 2023.
6. College of American Pathologists. CAP Guidelines. cap.org/protocols-and-guidelines/cap-guidelines. Accessed July 12, 2023.

illumina®

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

M-GL-01959 v1.0