Illumina Proactive | data security sheet

Enable the secure remote data performance service that allows our support teams to remotely diagnose, troubleshoot, and fix instrument issues.

Introduction

Reliable instrument operation is crucial for your lab. Illumina Proactive is a remote, secure instrument support service that helps to minimize unplanned downtime. When a sequencing run fails, it costs your lab time, labor, sequencing reagents, and samples. By leveraging only instrument performance data (Table 1), Illumina Proactive helps prevent this from happening. Our service and support team can remotely diagnose, troubleshoot, and fix issues, often before they are noticed. You'll also be able to schedule required component replacements as needed at your convenience (Figure 2).

Data security

Data security is a top priority for Illumina and our customers (Table 2).[1] As a result of consistent effort, security postures for Illumina products evolve overtime as new systems are designed and new threats to information are identified

Data privacy

The Illumina Proactive instrument support service is not able to access genomic data (sequencing run data), personally identifiable information (PII), or protected (patient) health information (PHI) (Figure 3). Only instrument performance data, run performance data, instrument configuration data, and run configuration data, are sent by the instrument to Illumina in a secure data stream (Figure 1).

Figure 1: Illumina Proactive secure data flow—The flow of instrument performance data collected by Illumina Proactive, from the instrument to Illumina and out to you the customer is secured through various administrative, physical, and technical controls to ensure data privacy.[1]

Detection	Engagement	Service	Result
Hardware concern is detected by Illumina Proactive	Illumina support team coordinates maintenance plan	Instrument is repaired and returned to service	Project is back online with little to zero sample loss

Figure 2: Illumina Proactive instrument service and support overview—Illumina Proactive service and support begins with detection of a hardware concern, followed by engagement with the Illumina support team to diagnose and fix the problem or schedule a repair or maintenance service, if needed. The result is reduced instrument downtime and potential loss of time, labor, and sample.

Information Collected		Information NOT collected	
✓ Optical System	✓ Thermal System	✗ Genomic data	
✓ Mechanical System	✓ Fluidics System	✗ Patient Health Information	

Figure 3: Data collected by Illumina Proactive—Illumina Proactive only collects data about general instrument health and performance and does not collect genomic data or patient health information.

Table 1: Data details and benefits

Instrument performance data	Run performance data	Instrument configuration data	Run configuration data
Data collected	Q-scores, instrument operational logs	Instrument serial number, software version	Run parameters, reagent, and flow cell lot numbers
Value to Illumina service team	Failure prediction, failure detection	Run troubleshooting	Run troubleshooting
Value to user	Enables analysis of error and warning notifications regarding optical, mechanical, thermal, and fluidic system performance	Enables assessment of whether software version, instrument type, or other hardware variables may be contributing to performance issues	Informs on roles of lot numbers, experiment type, and other experimental variables that contribute to performance issues

Table 2: Data security considerations with Illumina Proactive

Instrument performance data	Description		
Data NOT collected	**Sequencing run data, personally identifiable information (PII), or protected health information (PHI)**		
Privacy and security controls	Illumina uses administrative, physical, and technical controls to ensure data privacy[1]		
Inbound ports	No inbound ports from the internet are required for Illumina Proactive		
Data center security	Illumina leverages AWS data center security		
Data encryption at rest	AES-256	**HIPAA-Compliant Data Center**	Yes
Data encryption in transit	TLS	**GDPR-Compliant Data Center**	Yes
Software restriction policy (SRP)[a]	SRP limits the applications run on Illumina computers to those that Illumina has approved (allow-listed). SRP prevents any malware from being executed, even if it infiltrates the system		
Enhance machine experience toolkit (EMET)[b]	EMET is additional, complementary defense tool for Microsoft Windows. EMET is placed between the firewall and user-selected antivirus software and can be used to adjust Windows security features		

a. Available on the NovaSeq™ 6000 System and iSeq™ 100 System
b. Available on the NovaSeq 6000 System
Abbreviations: PII, personally identifiable information; PHI, protected health information; AWS, Amazon Web Services; AES, advanced encryption system; TLS, transport layer security; HIPAA, Health Insurance Portability and Accountability Act; GDPR, general data protection regulation.

Data security and regulatory considerations

Illumina Proactive integrates with the preexisting Illumina cloud infrastructure provided by Amazon Web Services (AWS),[3] and inherits controls that have allowed BaseSpace™ Sequence Hub to achieve ISO 27001 and Health Insurance Portability and Accountability Act (HIPAA) compliance. Data are encrypted at rest with Advanced Encryption System (AES)-256 and in transit through Transport Layer Security (Table 2).[4]

Illumina software as a service (SaaS) products are designed and operated in keeping with best practices and laws around data protection and data handling, including General Data Protection Regulation (GDPR).[5] Customers should determine GDPR responsibilities for use of their own personal data.

Note: Illumina Proactive does not require a BaseSpace Sequence Hub account.

Learn more

Learn more about Illumina Proactive Service at www.illumina.com/services/instrument-services-training/product-support-services/instrument-monitoring.html

Enabling Illumina Proactive

Initial setup and configuration of your network environment may require assistance from your IT department. After setup is complete, taking advantage of remote support with Illumina Proactive takes only a few seconds to activate. To connect an instrument to Illumina Proactive, use the instrument control software and simply check the box next to "Send Instrument Performance Data to Illumina" in the instrument control software settings before starting a run. The instrument performance data collected by Illumina Proactive remains secure both in transit and at rest. Sequencing run data, PII, or PHI are never included. If you have questions about enabling Illumina Proactive on your instruments, contact your local field applications scientist (FAS), field service engineer (FSE), or email our technical support team at techsupport@illumina.com.

References

1. Illumina (2018) Illumina Proactive Technical Note. Accessed July, 2019.
2. Microsoft Security TechCenter. Accessed July 2019.
3. AWS: ISO 27001. Accessed July 2019.
4. Announcing the Advanced Encryption Standard (AES). Accessed July 2019.
5. IBM: Transform your business with the GDPR. Accessed July, 2019.

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

illumina®