Commitment to Cybersecurity

Illumina is a leading developer, manufacturer, and marketer of life science tools and integrated systems for large-scale analysis of genetic variation and function. Because our technologies and services inherently involve handling large amounts of genomic and health data that must be well protected, cybersecurity is integral to our mission to improve human health by unlocking the power of the genome.

Innovations in data science and technologies are changing the world we live in. With the large-scale analysis of genomic data, scientists can better identify rare and undiagnosed diseases, shortening the diagnostic odysseys of patients around the world. Next generation sequencing technology is also accelerating the discovery of variants associated with cancer and enabling greater insights into infectious disease research, among many other applications. As more genomic and health data are collected and the number of people and technologies that process that data grows, cybersecurity practices that ensure the safety and integrity of data – and the individuals it comes from – are essential.

Illumina is committed to protecting the confidentiality and security of all personal information and data that are processed by our products, services, and business operations. Guided by our principles of Responsible Stewardship and Accountability, our Commitment to Cybersecurity highlights the five pillars of Illumina's cybersecurity program:

Program Governance

Strong governance is foundational for a successful cybersecurity program.

Illumina's cybersecurity program is championed by executive leadership. Our Board of Directors and senior management team are updated at least quarterly on cybersecurity program details and roadmaps to ensure appropriate allocation of capability and investment to achieve our regulatory and business objectives in a compliant manner. The cybersecurity program is reviewed annually by internal teams and independent third parties to assess our alignment with the NIST Cybersecurity Framework. Illumina always aims to hire and train exceptional cybersecurity professionals and all current cybersecurity team members hold at least one security certification, ensuring a broad set of expertise within the team.

Partnering with Industry

We believe creating partnerships and sharing knowledge are fundamental to advancing cybersecurity.

Illumina participates in the Healthcare Information Sharing and Analysis Center (H-ISAC), which provides cybersecurity resources to healthcare manufacturers and care providers. We also have a strong relationship with the Domestic Security Alliance Council (DSAC), a joint FBI and private sector information sharing forum. Our cybersecurity team members are frequent speakers in the cybersecurity community and are leaders in peer-based community programs to support cybersecurity, including the Information

Systems Security Association (ISSA), Society for Information Management San Diego (SIM), Chief Information Security Officer Roundtable, and InfraGard. Illumina understands the value in sharing our institutional knowledge with our cybersecurity colleagues and welcoming input from industry and governmental experts in return.

Secure Product Design and Placement

Mitigating risk at the earliest stages of product design and placement is integral to Illumina's cybersecurity program.

During the product development process, security design requirements are built into Illumina instruments and devices to ensure that products are robust and hardened from attacks. For instance, our product operating systems are designed to have reduced attack surfaces and user access levels appropriate for the function of the machine without compromising the security of the data. We thoroughly assess the security of all new instrument designs so that Illumina can have confidence in our instruments' integrity once installed at customers' locations.

For cloud-based products, Illumina uses a privacy by design approach that ensures customers' sensitive data is protected with strong encryption standards and strict controls for data access. Our cloud software products align with ISO 27001 and ISO 27034 standards. By aligning with these standards, Illumina performs secure design and architecture reviews, risk assessments, testing of software for security defects, and monitoring for vulnerabilities. These activities are a crucial and ongoing part of Illumina's Secure Development Lifecycle.

Risk Analysis and Security Testing

With persistent risk analysis and security testing, we can continue to improve the cybersecurity of all our products and practices.

Illumina continually assesses the cybersecurity risk environment and the posture of our instrument install 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 undergoes static analysis for security defects on a regular basis. Illumina also uses both internal and external penetration testing experts to validate our existing cloud software products on an annual basis, a key component of our Secure Development Lifecycle.

Data Protection

We protect data in compliance with all applicable laws and cybersecurity best practices.

Illumina's approach to data privacy and data protection strictly aligns with standards set by the GDPR, CCPA, HIPAA, other localized laws and regulations, and our Privacy Policy. As an enterprise, we provide robust capabilities for access management to realize a 'least-privilege' access model. Our backup capabilities encrypt and store data in immutable formats to provide for both confidentiality and integrity of data. Illumina CLIA laboratories ensure data quality and security through alignment with CLIA and regular HIPAA framework assessments.