White Paper

Agilent
Trusted Answers

Agilent Clinical Informatics Platform Security

Author

Maxim Tryhoen
Agilent Technologies Belgium S.A./N.V.

Overview

Data security, privacy, and their various aspects, such as availability, integrity, and confidentiality, are of critical importance to our customers. Agilent commits to delivering the highest quality services to our customers, addressing security at all stages of the product development life cycle.

This White Paper explains how the Agilent Alissa Clinical Informatics Platform implements security measures that comply with assorted U.S. and international regulations and standards. We have defined a set of policies, processes, and controls for security and privacy in accordance with the internationally accepted ISO 27001 and 27002 security standards.

The document is divided into three sections:

- The platform architecture and implementation that enable us to deliver the highest level of security and to comply with the regulations
- The security measures we have deployed to ensure data availability, data integrity, and data confidentiality
- The applicable data privacy regulations and how we comply

Introduction

The Agilent Alissa Clinical Informatics Platform is a Software as a Service (SaaS) product. The tools included in the Agilent Informatics Genomics area are delivered as services; the entire solution, from hosting to software application, is operated by our teams.

The infrastructure supporting our SaaS solution is Amazon Web Services (AWS). We chose to host our platform in AWS data centers for the following reasons:

- Highly secured data centers
- Geographically spread-out infrastructure to store data close to the customer and improve performance and end-user experience
- High availability, thanks to fully redundant hardware
- Commitment to security standards and regulations

The Agilent Alissa Clinical Informatics Platform is deployed in a layered architecture, as depicted in Figure 1.

Customers can access the platform's web applications using a web browser and a secure, encrypted connection. After connections have been filtered by the firewall, users must authenticate to access the Agilent Alissa Clinical Informatics Platform's various applications.

The platform leverages AWS features for administrator access, file storage, and logging. All AWS services in use are designed for high availability. The backend environment is not accessible from the internet. This backend environment contains the databases, including those storing patient information and the compute servers used to execute bioinformatics pipelines.

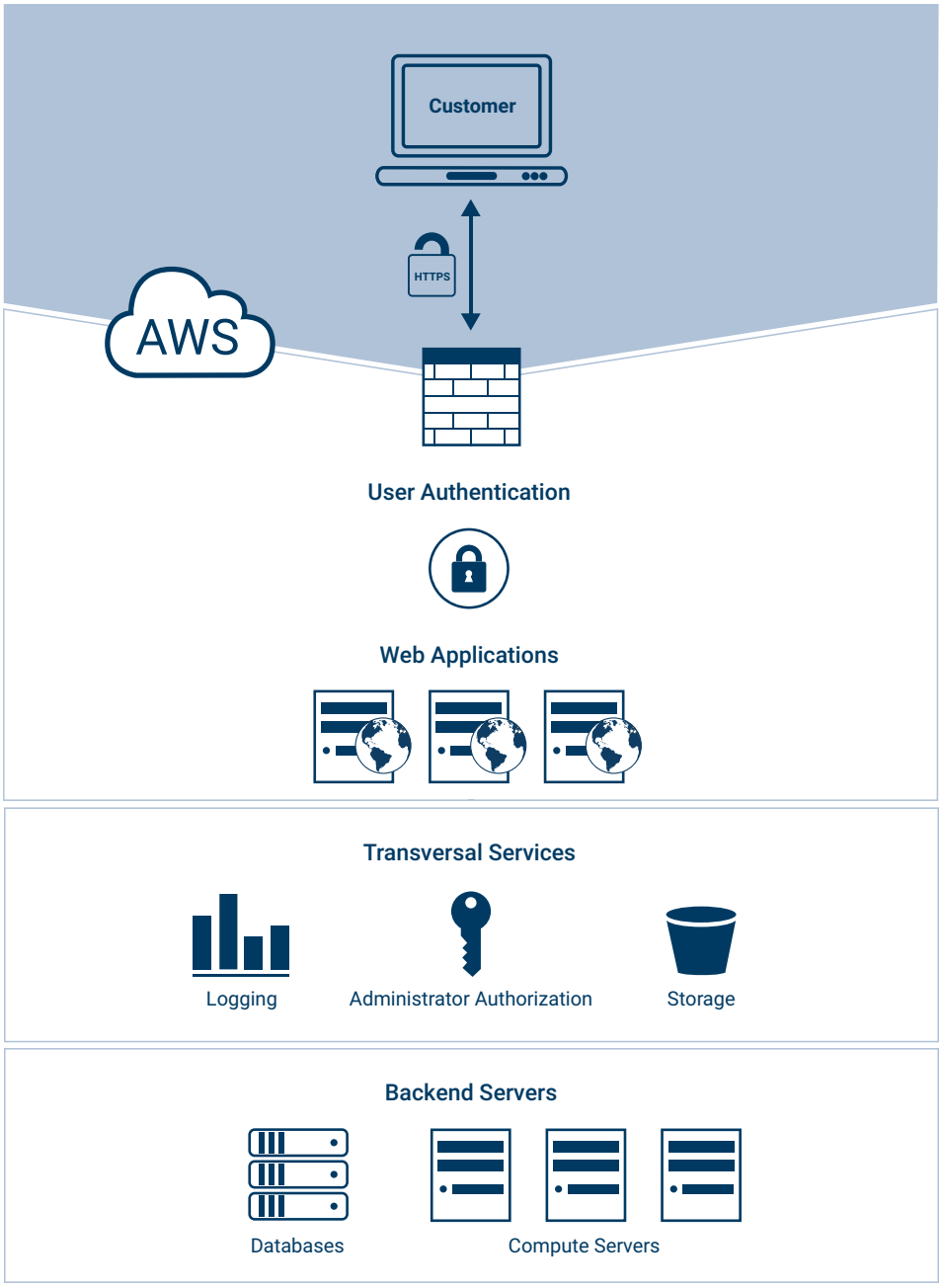

Figure 1. The secure layered deployment architecture of the Agilent Alissa Clinical Informatics Platform.

Security measures

This section details the measures taken by Agilent to address the main aspects of data security:

- **Availability:** To ensure that authorized users have prompt access to information when they need it
- **Integrity:** To safeguard the accuracy of information and the methods used to process it
- **Confidentiality:** To ensure that information is accessible only to those who need it
- **Auditability:** To keep evidence of all events for root-cause analysis

Regulations and compliance

Agilent software teams work with security experts to ensure that our SaaS products are compliant with international regulations, and that they help our customers comply with international standards.

Markets in which we are most active are: Europe, United States, Australia, and Canada. The applicable regulations in these markets include: GDPR, HIPAA, the Australian Privacy Principles, and PIPEDA. The international standard for information-security management is ISO 27001.

Availability

Security feature	Implementation
Facilities	AWS data centers demonstrate a strong physical security process, as acknowledged by their ISO 27001, ISO 27018, SOC1, SOC2, and SOC3 certifications.
Backup/restore	All AWS features used to store data (S3, EC2, EBS, RDS) are backed up and replicated in different data centers; restore tests are performed at least once a year.
Disaster recovery	A disaster-recovery plan is in place based on synchronous replication of the data and a strong backup/restore strategy for recovery in case of a major incident.

Integrity

Security feature	Implementation
Public key Infrastructure	All communications between customers and the applications or within the applications themselves are encrypted using 256-bit encryption, and signed by certificates delivered by an official certificate authority (CA).
Hardware checks	All hardware underlying AWS services is permanently checked for failures, and proactive migrations are performed.
Malware detection	All files uploaded in the platform are scanned for viruses, and compared to an up-to-date database of virus definitions.
Intrusion detection	Continuous scanning of incoming and outgoing traffic is performed with AWS Guard Duty, which triggers alarms in case of suspicious events.

Confidentiality

Security feature	Implementation
Authentication	Users must authenticate to a central login application and receive a session-based token; a password policy is in place to avoid weak passwords, and multifactor authentication can be enabled.
Authorization	All users and administrators have specific access rights based on the least-privilege principle.
Intrusion detection	Protection against DDoS and brute-force attacks is in place; vulnerability scanning is performed prior to product release to identify any potential security breach.
Encryption	All data in transit or at rest are encrypted using 256-bit encryption for data in transit and AES-256 for data at rest.

Auditability

Security feature	Implementation
Logging	All user and administrator actions are centrally logged and regularly reviewed; audit logs are accessible directly from the user interface, and logs are stored for 10 years.
Change management	All application changes or infrastructure changes go through a process that guarantees multiple levels of review before implementation.
Incident management	All incidents, minor or major, are centrally logged; a root-cause analysis is performed to improve overall security, and any incident involving patient data is communicated to the customer and to the appropriate authority, if required by law.

GDPR

In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) replaced the 1995 EU Data Protection Directive (European Directive 95/46/EC).

Agilent has a comprehensive GDPR compliance program and provides a processing solution that incorporates the relevant GDPR requirements and that allows a customer to be assured that in choosing Agilent they are making a GDPR compliant choice. To facilitate our global business, we adhere to the requirements for safeguarding transfers of personal data internationally, including through the use of Standard Contractual Clauses. Agilent personnel receive training on the GDPR and Agilent's obligations as both a data controller and a data processor to our customers.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, established requirements for the protection and security of patient health information held by Covered Entities and Business Associates in the United States. HIPAA was expanded by the Health Information Technology for Economic and Clinical Health (HITECH) Act, as incorporated in the American Recovery and Reinvestment Act of 2009, to address increasing reliance on electronic maintenance and storage of patient health information.

The requirements of HIPAA/HITECH are contained in rules that include the:

- **Privacy Rule:** Protects the privacy of Protected Health Information (PHI) in any form (that is, written, recorded, spoken orally, or electronic).
- **Security Rule:** Sets forth standards for the security—that is, the confidentiality, integrity, and availability—of PHI maintained in electronic form (known as ePHI) only.
- **Breach Notification Rule:** Requires Covered Entities and Business Associates to provide certain notifications following breaches of unsecured PHI.

Risk analysis on the Agilent Alissa Clinical Informatics Platform is performed in compliance with the requirements included in the HIPAA regulation, and the cloud infrastructure was built to support HIPAA-compliant services.

Where Agilent is a Business Associate, we partner with our Covered Entity customers to ensure that appropriate, HIPAA-compliant agreements and controls are in place.

APPs

The Australian Privacy Principles (APPs), which are contained in the Privacy Act 1988, outline how organizations must handle, use, and manage personal information.

The measures described in the Security measures section of this White Paper facilitate compliance with requirements of the APPs that apply to SaaS products.

PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian law relating to data privacy. It rules how organizations collect, use, and disclose personal information while doing business.

To comply with the 10 principles described in PIPEDA, Agilent regularly reviews a checklist of all the requirements. To meet the security-process requirements, security measures and regular controls and audits are in place.

ISO 27001

ISO/IEC 27001:2013 is an information-security standard that controls the following aspects of the security-management system of a company:

- Information-security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information-security incident management
- Information-security aspects of business continuity management
- Compliance with internal requirements such as policies, and with external requirements such as laws

The products under Agilent Alissa clinical informatics platform have been ISO 27001:2013 certified by an independent auditor for the full scope of its activities, which includes development, management, and support of a cloud-based platform for processing genomics data.

- Alissa Interpret is marketed in the US as a Class I Exempt Medical Device, in Europe as a CE IVD, and in Canada and Australia as a Class I IVD Device.

Glossary

AWS	Amazon Web Services
DDoS	Distributed Denial of Service
EBS	Elastic Block Storage
EC2	Elastic Compute Cloud
ePHI	Protected Health Information in electronic form
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
ISO	International Organization for Standardization
PHI	Protected Health Information
PIPA	Personal Information Protection Act
PIPEDA	Personal Information Protection and Electronic Documents Act
RDS	Relational Database Service
S3	Simple Storage Service
SaaS	Software as a Service
SOC	System and Organization Controls

Legal disclaimer

This White Paper is for general information purposes only, and should not be relied upon for the purposes of entering into legal relations with Agilent. All information in this White Paper is presented without any representation, guarantee, or warranty whatsoever regarding the accuracy, relevance, or completeness of the information. Agilent accepts no liability for any loss, claims, or damages as a result of any party relying on the general information set out in this White Paper.

www.agilent.com/lifesciences/alissa

For regulatory status of the Alissa products listed, please visit us at www.agilent.com/en/products/software-informatics/clinical-informatics-(alissa-platform)

This information is subject to change without notice.

Printed in the USA, August 31, 2023
5994-0125EN
PR7001-1454

Agilent
Trusted Answers