TECHNICAL NOTE

Illumina Connected Analytics로 보안, 프라이버시 및 규정 준수 요건 충족

높은 데이터 프라이버시 및 보호 기준에 부합하는 플랫폼

- 사이버 보안을 위한 Illumina의 조치와 고객의 책임
- Illumina Connected Analytics(ICA) 인프라의 보안 조치
- 국제 데이터 보호·프라이버시 표준 및 인증 준수
- 국제 데이터 보호·프라이버시 법률 및 규정 준수

illumina®

소개

차세대 시퀀싱(next-generation sequencing, NGS) 기술의 발전으로 데이터 생성량이 크게 증가하면서 데이터 분석 및 해석에 어려움이 발생하고 있습니다. Illumina Connected Analytics(ICA)는 인포매틱스(informatics) 워크플로우의 운영과 과학적 통찰의 도출을 위해 개발된 안전한 유전체 데이터 플랫폼입니다. ICA는 워크플로우의 효율성을 극대화할 수 있는 다양한 레스트풀 API(RESTful application programing interface, RESTful API)와 커맨드 라인 인터페이스(command-line interface, CLI) 도구를 갖춘 확장형(extensible) 플랫폼을 제공합니다. 이 플랫폼은 관련 현지/국제 규정과 기준의 요구 사항을 준수하도록 개발되었습니다. ICA는 정교한 유전체 데이터 플랫폼과 검증된 타사 보안 도구를 결합하여 환자 유래 유전체 데이터와 같은 민감한 정보를 다루는 고객의 엄격한 보안 요구 사항을 충족합니다. 본 문서는 어떻게 ICA가 보안 요구 사항과 관련 데이터 보호 법률 및 규정의 요구 사항을 준수하도록 개발되었는지를 자세히 기술합니다.

ICA의 보안 조치

높은 수준의 민감한 인간 유전체 데이터 보호를 위해 광범위한 보안 조치가 사용되었습니다. ICA는 데이터를 보안하고, 규정 준수를 염두에 두고 설계되었으며, ISO 27001과 ISO 13485를 비롯한 국제 표준을 준수합니다. 또한 기관과 기업의 세분화된 액세스(fine-grained access)를 통제하며, 데이터가 클라우드에서 처리되거나 인터넷을 통해 전송되거나 유휴 상태(at rest)로 저장되는지와 상관없이 플랫폼 전체에 걸쳐 데이터 흐름의 무결성(integrity)을 보장합니다. ICA는 환자의 기밀 정보를 수용하기 위해 다층적인 데이터 보안 기능을 제공합니다(표 1).

ICA는 안전한 클라우드 환경에 배포되므로 최고 수준의 격리(isolation)가 가능합니다(그림 1). 분석 파이프라인은 플랫폼에서 설정한 경계 내에 머물도록 하기 위해 컨테이너 내에서만 실행됩니다(데이터 액세스와 자원 소비 포함). ICA는 이를 통해 성능 저하 없이 강력한 플랫폼과 인프라 보안을 제공할 수 있습니다.

종합적인 플랫폼 보안 아키텍처

ICA는 임상, 제약 또는 연구 분야의 개인이나 기업을 위해 확장성이 뛰어난 고성능 데이터 처리 및 보관 역량을 지원합니다. 또 Illumina 시퀀싱 기기와의 안전하고 원활한 통합을 바탕으로 ICA로의 데이터 수집 절차가 간소화됩니다. 전송 중(in transit) 데이터와 유휴 상태의 데이터는 보안 조치를 통해 보호됩니다.

전송 중 데이터

ICA는 웹 기반 API를 통해 시퀀싱 기기와 통신합니다. 모든 시퀀싱 기기와 ICA 간 트래픽(traffic)에는 인터넷을 통해 전송되는 민감한 데이터를 암호화하는 표준 프로토콜인 전송 계층 보안(transport layer security, TLS 1.2)이 사용됩니다. 모든 서비스 방식에는 API 키가 요구되며 API 키 없이는 서비스가 제공되지 않습니다. 무분별한 요청을 방지하기 위해 요청은 모니터링됩니다.

유휴 시 암호화

ICA의 고객 데이터는 고급 암호화 표준(Advanced Encryption Standard, AES)인 AES-256을 사용하여 유휴 시 암호화됩니다.

네트워크 취약점 예방

경계 통제(boundary control) 기능은 네트워크 외부 경계와 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. 경계 통제 기능은 규칙 집합(rule set), 액세스 통제 목록(access control list, ACL) 및 구성(configuration)을 사용하여 정보가 특정 정보 시스템 서비스로 흐르도록 합니다. 트래픽의 흐름을 제어하기 위해 ACL 또는 트래픽 흐름 정책(traffic flow policy)이 관리형 인터페이스(managed interface)마다 설정됩니다.

다음과 같은 통제 기능이 추가적으로 제공됩니다.

- 타 보안 업체의 정기적인 침투 테스트(penetration test)
- 정기적인 네트워크 스캐닝
- 악성 코드(malware)가 포함된 첨부 파일로 인한 위험을 완화하는 데이터 이메일 전송 금지 정책
- 알려진 고정된 이미지로 배포된 시스템 호스트, 즉 가상 인스턴스(virtual instance)
- Open Web Application Security Project(OWASP)의 가이드라인에 따른 자동화된 안전한 코드 스캐닝
- 네트워크 및 호스트 기반의 탐지적(detective) 보안 통제와 예방적(preventive) 보안 통제

표 1: ICA의 데이터 보안 수준

보안 통제	ICA 기능	장점
로그인 정책(Login Policies)	관리자(admin)가 비밀번호 요구 사항 및 세션 종료 전 비활성 상태 유지 시간을 통제함.	높은 수준의 기밀성(confidentiality)을 제공함.
객체 소유권(Object Ownership)	기본적으로 모든 객체[b]는 플랫폼에 해당 객체를 처음 도입한 사용자가 소유권을 가짐. 객체[b]의 소유자는 소유자 권한(privilege)으로 다른 사용자, 회사 및 커뮤니티의 객체에 대한 세분화된 엑세스를 통제함.	세분화된 액세스 권한을 부여함.
감사 로깅(Audit Logging)	플랫폼 내 객체에 대한 작업(action)을 기록함.	규정 준수를 염두에 두고 설계함.
역할 기반 액세스 (Role-based Access)	클라이언트 관리자는 포괄적인 매트릭스를 통해 조직의 요구 사항에 부합하는 세부적인 보안 정의(definition)를 작성할 수 있음. 세분화된 보안 통제는 플랫폼 내에서 누가 무엇을 할 수 있는지를 엄격하게 규제함. 이는 모든 객체[b]에 적용됨.	관리자가 조직의 통제 요구 사항을 적용 가능함.
공개 키 기반 구조 (Public Key Infrastructure, PKI)	디지털 인증서, 공개 키 암호(cryptography) 및 인증 기관(certification authority)을 전사적인 네트워크 보안 아키텍처에 통합함. 이 프레임워크를 통해 공개 키 인증서의 생성, 생산, 배포, 제어, 계정 관리 및 폐기가 실행됨.	디지털 서명 및 암호화 기능을 제공함. 플랫폼 전체에 흐르는 데이터의 무결성[b]을 보장함.
데이터 암호화(Data Encryption)	모든 전송 중인 데이터는 TLS를, 유휴 상태인 데이터는 AES-256/128을 사용하여 암호화됨. 데이터의 무결성은 데이터를 다운로드하거나 파이프라인에 업로드하는 등의 작업을 수행하기 전에 검증됨. 데이터 침해(breach) 발생 시 ICA 보안 책임자에게 전달되고 해당 데이터가 격리됨. 근본 원인 확인 후 적절한 조치가 취해짐.	전송된 데이터를 숨기고 권한이없는 사용자는 해당 데이터를 읽을 수 없도록 하여 개인 정보의 기밀성을 지키는 데 사용됨.
2단계 인증 (Two-factor Authentication)[c]	민감한 작업[a]을 위한 단계별 인증 방식	보안층을 추가한 계정 액세스를 제공함.

a. 민감한 작업으로는 파이프라인의 변경, 데이터 업로드 및 구성 등이 포함됨.
b. 데이터는 데이터 세트와 파이프라인으로 정의되며, 객체는 데이터베이스 내의 모든 기록으로 정의됨.
c. Enterprise 고객 전용.

그림 1: 단일 샘플 및 인구 수준의 워크플로우를 지원하는 ICA

주요 기능

1. 워크플로우 내에서 투명하고 효율적으로 데이터를 업로드하고 처리할 수 있도록 시퀀싱 기기와 인프라에 원활하고 안전하게 통합이 가능합니다.

2. 버전 관리된 데이터 분석을 실행하는 고도로 구성 및 확장 가능하고 유연한 파이프라인을 제공합니다.

3. 파이프라인의 병렬 처리(parallel processing)를 통해 원할 때 언제든지 확장 가능한 데이터 분석이 가능하므로 데이터 분석 요구가 급증할 경우에 대비할 수 있습니다.

분석 파이프라인은 처리 소요 시간, 대기 시간 또는 효율성에 영향을 주지 않고 대용량 데이터 세트를 스트리밍하고 일괄 처리하는 역량을 갖추고 있습니다. 플랫폼 내에서 관련 규정의 요구 사항을 모두 준수하면서 안전하고 암호화된 방식으로 대량의 데이터를 처리합니다.

글로벌 데이터 센터 배포

ICA는 글로벌 배포 모델을 통해 데이터 소스에 가까운 위치 안에서 데이터를 저장하고 전산 해석을 수행할 수 있으며, 각 지역의 관련 데이터 보호 법률 및 규정의 요구 사항에 따라 데이터를 지역에 저장할 수 있습니다(그림 2). 따라서 고객은 새로운 프로젝트를 시작할 때 위치를 선택할 수 있습니다. 또한 전 세계를 아우르는 전략적인 플랫폼 배포로 현재 지원되는 전 세계 리전 중 한 위치에서 데이터의 저장 및 처리가 가능합니다.

사용자는 Data Residency Control 기능을 이용하여 하나의 인터페이스로 전 세계에서 진행 중인 프로젝트를 관리하고 데이터를 처리할 수 있습니다. 여러 데이터 센터를 따로 관리할 필요 없이 안전하게 협업하고 데이터를 공유하면서 데이터 상주(data residency) 요구 사항을 충족할 수 있습니다.

뛰어난 데이터 가용성 및 통제

ICA에 높은 데이터 가용성(data availability)을 확보해 줄 수 있는 믿을 만한 데이터 센터 파트너사를 신중하게 선정하였습니다. 또한 Illumina는 ICA가 높은 보안 요구 사항을 충족하며 데이터 센터 내에서 운영될 수 있도록 적극적으로 지원하고 있습니다(표 2).

가용성

내외부 가용성 위험을 완화하기 위해 ICA는 비즈니스 연속성(business continuity) 및 재해 복구(disaster recovery) 계획을 포함하고 있습니다. ICA는 Uptime Institute의 Tier III 데이터 센터 설계 기준을 준수하는 ISO/IEC 27001:2013 인증을 획득한 시설에 있는 고가용성(high-availability) 클라우드 인프라에 설치됩니다.

데이터 보안 및 이중화(redundancy)는 두 데이터 센터에 걸쳐 액티브/패시브(active/passive) 방식으로 분산 구성된 중앙 플랫폼을 사용하는 사유 장애 조치(failover) 앱의 보호를 받습니다. 따라서 문제가 발생하면 중앙 플랫폼이 백업 노드(backup node)로 이동됩니다. 이러한 장애 조치의 복구 시간 목표(recovery time objective, RTO)는 6시간입니다. 복구 시점 목표(recovery point objective, RPO)는 0이며, 이는 프로덕션 데이터베이스를 백업 데이터베이스로 동기적으로 전송함으로써 즉시 충족됩니다.

무결성

ICA는 클라우드 기반 플랫폼 내에서 모든 작업을 실행하기 전에 데이터 무결성 확인을 위해 설계된 PKI를 사용하여 데이터의 무결성을 보장합니다.

기밀성

ICA는 가명 처리(pseudonymization)와 전송 중인 데이터(TLS 1.2 사용)와 유휴 상태 데이터(AES-256/128 사용)의 암호화를 통해 클라우드 환경에서 이루어지는 데이터 처리 활동의 기밀성을 우선으로 삼고 있습니다.

또 ICA는 데이터 암호화 외에도 필요한 액세스 통제를 적용하여 플랫폼에 대한 허가되지 않은 액세스를 제한합니다. 이로써 강력한 사용자 인증 메커니즘을 사용한 ID 및 액세스 관리로 기밀성을 한층 더 강화할 수 있습니다. 또한 데이터 처리 업체의 직원과 협력 업체도 기밀 유지의 의무가 있다는 의견이 있습니다.*

* 일부 통제자는 클라우드 서비스 제공 업체가 암호 키에 액세스할 수 없어 호스팅된 정보를 해독할 수 없는 영지식(zero-knowledge) 솔루션을 특정 정보에 적용하는 것을 고려해 볼 수 있습니다. 이 경우 기밀성 위험은 크게 감소하지만, 영지식 솔루션의 사용이 의무는 아닙니다. 추가적인 계약적, 조직적 안전 장치와 같이 기밀성을 보장할 수 있는 대안책을 마련해 볼 수도 있습니다.

그림 2: ICA의 전 세계 AWS 리전 데이터 센터 배포 현황

표 2: ICA 데이터 보안 요구 사항

보안 요구 사항	ICA 기능	장점
가용성	신뢰할 수 있는 데이터 센터와의 파트너십	전용 네트워크 연결, 이중화, 무정전 전원 공급 장치(uninterruptible power supply, UPS), 효과적인 데이터 백업 전략을 보장함.
무결성	PKI 인프라	플랫폼 전체에 걸쳐 데이터 흐름의 원본성(originality)과 무결성을 보장함.
기밀성	전송 중 데이터(TLS 1.2 사용)와 유휴 상태 데이터(AES-256/128 사용)의 암호화	데이터 기밀성을 보장함.
투명성	각 클라이언트의 데이터 보존 요구 사항 준수	데이터 센터의 위치를 공개함.
데이터 격리	업계 표준 데이터 분리(segregation) 기술	데이터가 실수로 제3자에게 공유/공개되지 않도록 함.
이동성(Portability)	표준화된 데이터 출력 도구	벤더 록인(vendor lock-in, 특정 벤더에 종속되는 현상) 없이 클라이언트 데이터를 내보낼 수 있음.
책임성(Accountability)	IT 책임성을 보장하는 메커니즘	모든 활동을 항시 기록함.

투명성

ICA는 대부분의 데이터 상주 및 프라이버시 요구 사항을 준수합니다. 데이터 센터 리전 및 제공 업체는 공개됩니다.

격리

ICA는 알 필요성(need-to-know)의 원칙 등 업계 표준 데이터 분리 기술을 기술적, 조직적 조치(예: 세분화된 보안 통제로 결정되는 역할 기반 액세스 통제)를 통해 적용하여 최고 수준의 데이터 격리를 제공합니다.

이동성 및 서비스 종료 후 데이터 관리

ICA에서 처리되는 데이터는 고객이 언제나 이용할 수 있습니다. 표준화된 데이터 출력 도구를 사용하면, 상호운용성이 부족하여 고객이 클라우드 서비스 제공 업체를 변경하지 못하거나 서비스를 내부 조달할 수 없는 상황, 즉 벤더 록인의 발생 위험이 없습니다.

기록 관리 및 감사 로그

ICA는 기록 관리와 감사 로그(audit log) 기능을 제공하므로 항상 플랫폼 내에서 모든 객체, 작업 및 활동(예: 객체 보기)의 IT 책임성을 보장합니다.

Illumina 보안 관행

Illumina의 사이버 보안 프로그램은 임원진의 지지를 받고 있습니다. Illumina의 이사회와 고위 경영진은 적어도 분기별로 사이버 보안 프로그램에 대한 자세한 정보와 로드맵을 보고 받음으로써 관련 법률과 규정에 따라 규제 및 사업 목표를 달성하기 위해 요구되는 역량과 투자가 적절히 할당되도록 하고 있습니다. 사이버 보안 프로그램은 미국 국립 표준 기술 연구소(National Institute of Standards and Technology, NIST)의 Cybersecurity Framework 충족 여부를 평가하기 위해 내부 팀과 독립적인 제3자 기관을 통해 매년 검토를 받고 있습니다. 또한 Illumina는 우수한 사이버 보안 전문가의 고용과 교육을 위해 노력하고 있습니다. 현재 사이버 보안 팀은 모든 팀원이 최소 한 개의 보안 인증을 보유하고 있어 팀 자체적으로 폭넓은 전문성을 지니고 있습니다.

제품 설계 단계에서의 위험 관리

보안 취약점을 최소화하기 위해 ICA와 Illumina의 제품 개발에는 보안 설계 요구 사항이 내재되어 있습니다. 예를 들어, Illumina 제품의 운영 체제는 데이터 보안에 대한 타협 없이 공격 표면(attack surface)은 줄이고 기기의 기능에 적합한 사용자 액세스 레벨을 낮게 설정하였습니다.

특히 Illumina는 클라우드 기반 제품의 경우 개인 정보 처리가 필요한 새로운 제품, 프로세스 또는 서비스의 개발 수명 주기 중 가능한 한 이른 시점에 프라이버시 통제 기능을 내장하고 프라이버시 위험을 해결하기 위해 Privacy by Design(프라이버시를 고려한 설계)을 실천하고자 최선을 다 하고 있습니다.

또 Illumina는 안전한 설계 및 아키텍처 검토, 위험 평가, 보안 결함 식별을 위한 소프트웨어 검사 그리고 취약점 모니터링을 수행합니다. 이러한 중요한 활동은 Illumina의 안전한 개발 수명 주기 중 지속적으로 진행됩니다.

위험 분석 및 보안 검사

Illumina는 업계의 파트너사, 고객, 지원팀과 협력하여 설치된 기기의 사이버 보안 위험 환경과 보안 상태를 지속적으로 평가합니다. 신제품은 진화하는 사이버 보안 위험과 위협에 대응하기 위해 높은 기준을 충족하도록 설계되며 최신의 전사적인 사이버 보안 관행의 적용을 받습니다.

Illumina는 또한 주기적으로 클라우드 소프트웨어 제품의 소프트웨어 코드 보안 검사를 진행합니다. 우선 표준 빌드(build) 절차의 일환으로 정기적으로 보안 결함을 확인하는 소프트웨어 코드 정적 분석(static analysis)을 수행하고 있습니다. 또한 매년 내외부 침투 시험 전문가가 안전한 개발 수명 주기의 핵심 구성 요소인 기존의 클라우드 소프트웨어 제품을 검증하고 있습니다.

Illumina 직원 보안 관행

Illumina는 전 세계 모든 채용 후보자에 대한 배경 조사를 실시합니다. 배경 조사에는 학력, 대학 학위, 고용 이력, 범죄 기록이 포함됩니다. 담당자는 문서화된 정책 및 절차를 통해 보안 위반을 방지하고 탐지하며 억제할 수 있고 서로의 상관관계를 파악할 수 있습니다.

ICA에 대한 기술 지원을 제공하는 직원들은 보안 인식 및 교육 프로그램을 통해 Illumina의 보안 정책을 숙지합니다. 자동 규정 준수 모니터링 시스템은 직원들의 교육 요건 준수 여부를 계속해서 확인합니다. ICA에 대한 기술 지원을 제공하는 모든 Illumina 직원들은 Illumina의 보안 정책 위반 시 징계 조치를 받을 수 있음을 알고 있습니다.

- ICA에 대한 기술 지원을 제공하는 모든 Illumina 직원들을 대상으로 매년 올바른 고객 데이터 취급 방법에 대한 교육을 실시합니다.
- 고객 데이터의 다운로드는 제한됩니다.
- 최소 권한(least privilege)의 원칙에 따라 ICA 액세스 권한은 필요한 경우에만 Illumina 직원에게만 부여됩니다. 즉, 직원이 업무 수행에 필요한 최소 수준의 권한만이 주어집니다.
- Illumina는 정기적으로 직원의 권한을 검토하고, 정당한 사유가 있는 경우 액세스 레벨을 변경합니다.
- 시스템 액세스는 자동 티켓팅 시스템에 기록되고 문서화됩니다.
- Illumina 퇴사 시 퇴사자의 프로덕션 환경, Illumina 앱, IT 시스템에 대한 액세스 권한은 취소됩니다. Illumina 소유의 장비와 배지도 모두 반환해야 합니다.

ICA 인증

ICA는 반드시 관련 데이터 보호, 보안 및 품질 요구 사항을 준수해야 하며 규제된 환경에서 운영해야 하는 고객에 적합한 제품입니다. IT는 Amazon Web Services(AWS)의 기존 클라우드 인프라에 구축되므로 몇 가지 AWS 표준 및 인가(accreditation)를 공유하고 있습니다(표 3). 또한 ICA는 ISO 27001, ISO 13485 등 다양한 국제 승인 표준을 준수합니다(표 3). ICA는 광범위한 데이터 보안 인증(data security certification)을 제공함으로써 고객의 관리적, 재정적 부담을 완화해 줍니다.

ISO 27001

ICA는 대량의 오믹스(omics) 데이터와 건강 데이터를 처리하는 클라우드 기반 분석 플랫폼의 개발, 관리 및 지원을 비롯한 모든 활동에 대해 독립된 감사인으로부터 ISO 27001 인증을 획득하였습니다. Illumina는 ISO 27001 요구 사항을 준수하는 정보 보안 관리 시스템(information security management system, ISMS)을 운영하고 유지합니다.

정보 보안 통제

- 보안 인식 및 교육
- 모니터링
- 액세스 통제 및 책임성
- 재해 복구 계획
- 인증
- 사고 대응
- 장비 유지 관리
- 안전한 미디어 취급
- 물리적, 환경적 보안 조치
- 위험 관리
- 시스템 및 네트워크 보안

ISO 13485

ICA는 Illumina 품질 관리 시스템(Quality Management System, QMS)의 소프트웨어 수명 주기(Software Life Cycle, SLC) 프로세스에 따라 개발되었습니다.

Illumina는 ISO 13485 요구 사항을 준수하는 QMS를 운영하고 유지하고 있습니다. QMS의 관리 범위에는 유전자 분석에 활용되는 유전형 분석(genotyping), 유전자 발현(gene expression) 및 PCR 관련 제품, 기기와 소프트웨어의 설계, 개발, 제조, 유통, 설치, 정비가 포함됩니다. 또한 Illumina의 QMS 내 프로세스에는 업계 모범 사례와 관련 표준(예: 위험 관리 프로세스는 ISO 14971, SLC 프로세스는 IE62304)이 적용되어 있습니다.

표 3: ICA 인증 및 인가

인증	설명
ISO 13485	의료 기기에 대한 국제 표준으로, 조직이 고객의 요구와 관련 규정 요구 사항을 일관성 있게 충족하는 의료 기기와 관련 서비스를 제공할 수 있음을 증명하도록 하는 QMS의 요건을 명시함.
ISO 27001	정보 관리 시스템을 갖추고 있음을 증명하는 ISO 27001 인증은 정보 보안 위험 관리에 대한 국제 표준으로, 프로세스 기반의 ISMS 구축, 구현, 운영, 모니터링, 유지 및 지속적인 개선을 요구함.
AWS 표준 및 인가	
Service Organization Controls 1/SSAE 16/ISAE 3402	고객 데이터를 보호하는 AWS 통제 항목이 제대로 설계되어 있는지, 또 개별적인 통제 항목이 효과적으로 운영되는지를 증명하는 감사
Federal Information Security Management Act(FISMA) - Moderate	연방 정보 시스템 보안 강화를 위한 미국 정부의 인가(예: NIH 데이터 센터 FISMA Moderate 등급 획득)
Payment Card Industry Data Security Standard - Level 1	전자 결제 보안 강화를 위한 표준으로, AWS는 최고 수준의 인증을 획득함.
Federal Information Processing Standard Publication 140-2	암호 모듈(cryptography module)의 요건을 명시하는 미국 정부의 컴퓨터 보안 표준

ICA 법률 및 규제 환경

Illumina는 관련 데이터 보호 및 보안 규정과 요구 사항을 준수하기 위해 노력하고 있습니다. ICA는 운영의 기밀성, 무결성 및 가용성을 유지하고 법적, 규정적 요구 사항(표 4)을 충족하는 데 필요한 보안 가이드라인과 통제 항목을 제공합니다.

CLIA 및 CAP

미국에 본거지를 두고 인간 샘플을 시퀀싱하는 고객은 1988년에 발표된 Clinical Laboratory Improvement Amendments(CLIA; 이하 CLIA 규정)[2]에 기술된 대로 Centers for Medicare and Medicaid Services(CMS)[1]의 관할하에 있습니다. CLIA 규정은 질병의 진단, 예방 및 치료, 혹은 건강 상태의 확인을 위해 인간 검체 대상으로 수행되는 실험실 검사의 품질 기준을 수립합니다.

또한 CLIA 규정은 검사 결과의 정확성, 신뢰성 및 적시성을 보장하도록 되어 있습니다. 규정에는 숙련도 시험, 검사 관리, 품질 관리, 담당자 자격 요건 그리고 품질 보증에 대한 품질 기준이 포함됩니다.

임상 검사실은 College of American Pathologists(CAP)[3]의 한층 더 엄격한 기준에 따른 평가를 받을 수도 있습니다. 규정 측면에서 보자면, CAP 기준은 CLIA 규정의 요구 사항보다 더 엄격한 것으로 인정받고 있습니다. 이에 따라 CMS는 공식적으로 CAP 인가 획득 시 CLIA 규정 준수도 함께 인증된 것으로 간주합니다.

ICA의 CLIA/CAP 지원

CLIA 및 CAP 검사실에서는 ICA를 사용하여 데이터를 보관, 관리, 분석할 수 있습니다. ICA는 다음과 같이 검사실에서 데이터 무결성, 정확성 및 신뢰성을 위해 활용해 볼 수 있는 몇 가지 기능을 제공합니다.

- 시퀀싱 기기에서 업로드된 데이터는 소스 데이터의 무결성을 보증하기 위해 확인 절차를 거칩니다.
- ICA의 도구와 파이프라인은 버전 관리를 하며, 수정 방지 절차가 마련되어 있습니다.
- 결과의 해석을 바꿀 수 있는 기능은 버전을 명명하여 새로운 검증 과정이 완료될 때까지는 이전 버전이 사용되도록 합니다.
- 수행된 모든 분석에 대한 설명이 상세 로그를 통해 제공됩니다.

GDPR

ICA는 일반 데이터 보호 규정(General Data Protection Regulation, GDPR)의 근간인 프라이버시 원칙에 부합하도록 개발되었습니다. Illumina는 제품의 설계와 아키텍처에 기술적, 조직적 조치를 적용하여 고객이 ICA에서 처리되는 개인 데이터, 그중에서도 특히 유전체 데이터와 같이 특수한 범주의 개인 데이터를 보호할 수 있도록 합니다.

ICA는 주요 릴리스가 있을 때마다 프라이버시 위험을 식별하고 식별된 위험을 적절히 완화하기 위해 내부적으로 프라이버시 평가를 실시하고 있습니다. 또한 Illumina는 고객과 수탁 처리 업체와의 계약을 통해 각 당사자의 GDPR 의무를 충족합니다.

HIPAA

ICA는 보안 규칙(Security Rule) 및 프라이버시 규칙(Privacy Rule)에 따라 관리적, 기술적 통제를 이행하는 등 건강보험 양도 및 책임에 관한 법률(Health Insurance Portability and Accountability Act, HIPAA)의 요구 사항을 준수하도록 설계되었습니다(표 5).

또한 고객, 즉 적용 대상 기관(covered entities)과 협력 업체와의 계약을 통해 Illumina는 각 당사자의 HIPAA 의무를 충족합니다.

PIPEDA

캐나다에서는 개인정보보호 및 전자문서법(Personal Information Protection and Electronic Documents Act, PIPEDA)에 따라 개인 정보 보호를 규제합니다. Illumina는 ISO 27001 인증을 위해 이행되었고 PIPEDA 가이드라인에도 기술되어 있는 통제 항목을 포함하는 정책과 절차를 적용하였습니다. 캐나다 프라이버시 커미셔너 사무소(Office of the Privacy Commissioner of Canada, OPC)는 위험 관리, 보안 정책, 인적 자원 보안, 기록 관리, 액세스 통제, 기술적 보안, 물리적 보안 등 합리적인 PIPEDA 안전 장치 준수를 감독합니다.

기타 데이터 프라이버시 법률 및 규정

ICA는 유럽 및 북미의 프라이버시 법률에 대응함으로써 대다수 Illumina 고객의 데이터 보호 의무를 충족합니다. 다만, 이 밖에도 데이터 프라이버시 법률과 규정이 새롭게 마련되고 발전되고 있기 때문에 Illumina는 이러한 법률의 준수를 위해 고객이 의무를 다 할 수 있도록 지속적인 ICA 업데이트를 통해 필요한 기능을 통합할 계획입니다.

표 4: ICA 규정 요구 사항

규정/요구 사항	설명
CLIA(미국)	질병의 진단, 예방 및 치료, 혹은 건강 상태의 확인을 위해 인간 검체 대상으로 수행되는 실험실 검사의 품질 기준을 수립하는 규정
CAP	CLIA 규정의 요구 사항보다 훨씬 더 엄격한 것으로 인정받는 기준
GDPR(유럽 연합)	유럽 연합(European Union, EU) 및 유럽 경제 지역(European Economic Area, EEA) 내 모든 이에 적용되는 유럽 연합의 데이터 보호 및 프라이버시 규정
HIPAA(미국)	미국에서 보호받는 의료 정보(protected health information, 즉 환자 데이터)를 처리하는 적용 대상 기관과 비즈니스 관계자(business associate)를 통제하는 법률
PIPEDA(캐나다)	영리 활동(commercial activity) 중 조직의 개인 정보 수집, 사용 및 공개를 통제하는 캐나다 연방 입법
DSPTK(영국)	건강 데이터에 적용되는 데이터 보호법인 Data Protection Act 2018하의 데이터 보호 법률을 포함하는 정보 거버넌스 기준(information governance standard)으로, 영국에서 GDPR을 보완하는 역할

DSPTK

영국 국민 보건 서비스(National Health Service, NHS)는 National Data Guardian의 10가지 데이터 보안 기준과 GDPR의 관련 항목에 따라 조직의 성과를 측정하고 발표하는 온라인 자체 평가 도구인 Data Security and Protection Toolkit(DSPTK)을 소개하였습니다. DSPTK는 Cyber Essentials Plus, ISO 27001 등 기타 인정받는 데이터 보안 모범 사례도 지원합니다. ICA는 영국 Data Protection Act 2018하의 데이터 보호 법률을 포함하는 현재 버전의 DSPTK 기준에 명시된 의무를 충족합니다.

고객 보안 통제

AWS의 공동 책임(shared responsibility) 모델과 마찬가지로 ICA를 사용하는 고객에게는 몇 가지 책임이 따릅니다. 고객은 서비스형 소프트웨어(software-as-a-service, SaaS) 솔루션의 사용을 설명하기 위한 위험 평가를 받아야 하며, 이러한 위험 평가 결과는 각 고객의 프라이버시 및 보안 통제 검토에 반영되어야 합니다. 예를 들어, 비밀번호 정책은 ICA 계정 및 비밀번호 공유를 금지해야 합니다. 기관은 액세스 승인 절차와 과정을 마련하고 정기적으로 모든 사용자에게 부여된 액세스 권한을 검토해야 합니다.

표 5: ICA의 HIPAA 보안 규칙 통제

보안 통제	설명
관리적 통제	• 보안 위반 방지, 감지, 억제 및 시정 정책과 절차 • 보안 정책 및 통제 항목의 개발과 구현을 책임지는 보안 담당자 • 직원의 적절하고 승인된 고객 데이터 액세스를 확인하는 절차 • 고객 데이터 액세스 권한 부여 과정 • 보안 정책 교육을 받은 직원 • 사고 보고 과정 • 데이터 보안에 영향을 미치는 환경적, 운영적 변화에 대한 주기적인 평가 • 모든 새로운 사용자 데이터 처리 기능에 대한 프라이버시 영향 평가(privacy impact assessment, PIA)
물리적 통제	• 시설 접근 통제 시행 • 안전한 데이터 센터 내 ICA 호스팅 • 작업 장소 보안 관련 정책 • 모바일 기기 관련 정책과 절차 • ICA 지원 기기 목록 유지
기술적 통제	• 고유한 사용자 ID • ICA 또는 고객사의 ID 관리 시스템을 통한 사용자 인증 • 전송 중 데이터의 무결성 보호 • TLS 기반 전송 중 데이터 암호화 • 사용자 개시 데이터 삭제 기능
ISO 27001 통제	• A.5 Information security policies(정보 보안 정책) • A.6 Organization of information security(정보 보안 조직) • A.7 Human resources security(인적 자원 보안) • A.8 Asset management(자산 관리) • A.9 Access control(액세스 통제) • A.10 Cryptography(암호화) • A.11 Physical and environmental security(물리적, 환경적 보안) • A.12 Operational security(운영적 보안) • A.13 Communications security(통신 보안) • A.14 System acquisition, development, and maintenance(시스템 획득, 개발 및 유지 관리) • A.15 Supplier relationships(공급 업체 관계) • A.16 Information security incident management(정보 보안 사고 관리) • A.17 Information security aspects of business continuity management(비즈니스 연속성 관리의 정보 보안 측면) • A.18 Compliance(규정 준수)

아울러 고객은 ICA로 처리하는 데이터의 내용을 포함하는 모범 사례를 검토하고 수립해야 합니다. 예를 들면, 명명 정책은 피험자 정보 식별의 도입을 금지해야 합니다. ICA 액세스에 사용되는 작업 장소에는 안티바이러스 소프트웨어, 호스트 기반 방화벽, 중앙 집중식 로깅(centralized logging) 등과 같은 적절한 보호 장치가 설치되어 있어야 합니다. 비즈니스 연속성과 재해 복구 계획은 ICA 사용을 설명하기 위해 업데이트되어야 합니다.

침해 통지

ICA 사용 고객은 침해로 인해 데이터 손상이 발생했을 수 있는 개인과 적절한 감독 기관에 이를 통지해야 할 책임이 있습니다. 여기에는 잘못된 로그인 시도, 로그오프, 다운로드, 보기, 공유가 포함됩니다. 로그에는 날짜, 시간, 사용자, 각 작업에 대한 설명이 포함됩니다. 데이터 수정의 설명에는 데이터 수정에 사용된 도구의 이름 또는 API 호출(call)이 제공됩니다. 사용자는 API를 통해 외부 시스템에서 감사 로그를 관리할 수 있습니다.

요약

ICA는 지속적인 NGS 기술의 발전으로 데이터 생성량이 증가하면서 대량의 데이터를 관리, 분석, 해석하기 위해 마련된 제품입니다. 연구, 임상 치료, 인간 진단을 위해 대용량 유전체 데이터를 보관하고 공유하기 위해서는 데이터 보안과 현지 및 국제 표준의 포괄적인 규정 준수가 필요합니다. ICA는 관련 데이터 보호·프라이버시 요구 사항에 따라 이러한 필요성을 충족하고, 대량의 유전체 데이터를 비교적 저렴한 비용으로 빠르고 효율적으로 처리할 수 있도록 개발되었습니다.

상세 정보

자세한 정보는 www.illumina.com/ConnectedAnalytics에서 확인하실 수 있습니다.

참고 문헌

1. Centers for Medicate and Medicaid Services. www.cms.gov. Accessed August 18, 2021.
2. Clinical Laboratory Improvement Amendments (CLIA). www.cms.gov/regulations-and-guidance/legislation/clia. Accessed August 18, 2021.
3. CAP Guidelines. www.cap.org/protocols-and-guidelines/current-cap-guidelines. Accessed August 18, 2021.

illumina®

무료 전화(한국) | 080-234-5300
techsupport@illumina.com | www.illumina.com

M-GL-00333 v2.0 KOR