NOTA TÉCNICA

Seguridad, privacidad y cumplimiento de Clarity LIMS™

Las características y la estrategia que ayudan a proteger sus datos

illumina®

Impulsar prácticas sólidas de seguridad y privacidad

La protección de la privacidad de la información médica protegida (PHI, Protected Health Information), incluidos los datos genómicos, es fundamental para las operaciones comerciales globales de Illumina. Nuestra estrategia de protección y privacidad de datos, articulada en nuestra Política de privacidad corporativa, se alinea con las normas clave establecidas por las normativas de privacidad de datos nacionales y globales, incluida la Ley de portabilidad y responsabilidad de seguros sanitarios (HIPAA, Health Insurance Portability and Accountability Act), el Reglamento general de protección de datos (RGPD) y la Ley de privacidad del consumidor de California (CCPA, California Consumer Privacy Act). Estamos comprometidos con los siguientes principios rectores:

- **Transparencia**: comunicamos claramente nuestras prácticas de privacidad y cómo utilizamos los datos personales.
- **Administración responsable**: protegemos los datos personales para mantener su confidencialidad y seguridad.
- **Uso ético**: solo recopilamos y utilizamos datos personales de forma legal y transparente para fines que promuevan nuestra misión de mejorar la salud humana al aprovechar todas las posibilidades del genoma.
- **Responsabilidad**: nos comprometemos a cumplir con todos los requisitos legales y a promover prácticas internas para lograr los más altos estándares de privacidad de datos personales.

Marcos de seguridad

Las prácticas de privacidad institucional sólidas se basan en un programa de seguridad de la información exitoso. Aunque existen varios marcos de seguridad en vigor a nivel mundial, nuestras prácticas y esta nota técnica se centran en los marcos más comunes, entre los que se incluyen:

- HIPAA
- International Organization for Standardization (ISO) 27001 (seguridad) y 27701 (privacidad)

Infraestructura

Illumina aplica sus propios controles y procedimientos de seguridad para la seguridad de Clarity LIMS (sistema de gestión de información de laboratorio) junto con un enfoque completo y probado de Amazon Web Services (AWS) (Figura 1).[1]

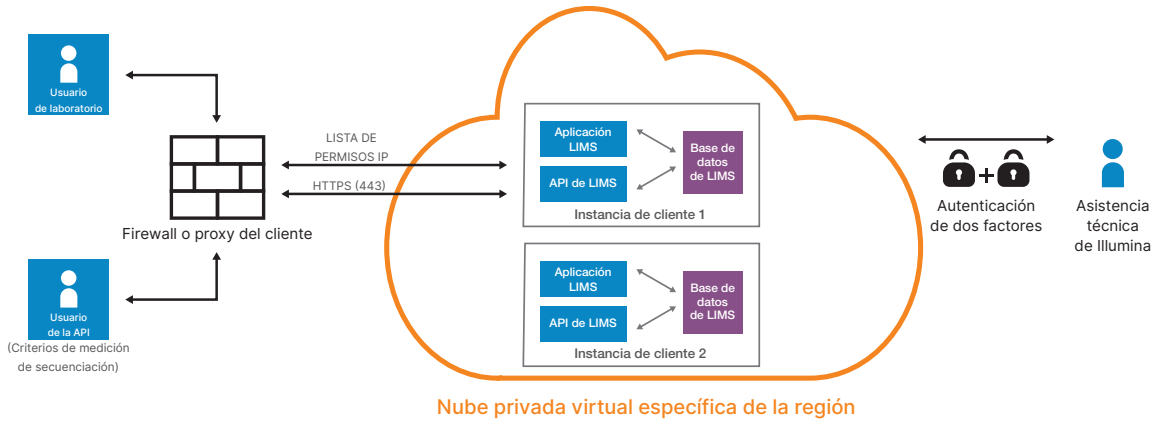

Figura 1: Infraestructura de seguridad del software Clarity LIMS.

Seguridad de un vistazo

En la Tabla 1, se proporciona una descripción general de alto nivel de los controles de seguridad incorporados en el software Clarity LIMS. En el resto de esta nota técnica, se proporciona información detallada.

Tabla 1: Lista de comprobación de privacidad y seguridad de Clarity LIMS

Internos y de procedimiento			
Comprobaciones de antecedentes de los empleados	✓	Supervisión	✓
Políticas de seguridad	✓	Respuesta ante incidentes	✓
Control de acceso	✓	Antimalware	✓
Acceso de solo lectura asignable al rol	✓	Planes de recuperación ante desastres	✓
Copias de seguridad	✓		
Aplicación en la nube			
Control de acceso	✓	Antimalware	✓
Cifrado en reposo	✓	Recuperación ante desastres	✓
Cifrado en tránsito	✓	Copia de seguridad de los datos	✓
Registro de actividad	✓	Integridad de los datos	✓
Prueba de intrusión de terceros	✓	Revisión/prueba del código	✓
Control de acceso basado en roles	✓	Red	✓
Controles de contraseña	✓	Segmentación de red	✓
Gestión de sesiones	✓		
Cumplimiento y certificación: versión 5.4 y posteriores			
ISO/IEC 27001:2013 (para instancias en la nube)	✓	HIPAA (validado por terceros)	✓
ISO/IEC 27701:2019 (para instancias en la nube, v6.1 y posteriores)	✓		

Prácticas de seguridad de los empleados

Nuestras prácticas de seguridad comienzan antes de que se incorporen nuevos empleados. Realizamos comprobaciones de antecedentes de todos los candidatos a empleados según lo permite la ley. Las políticas documentadas guían al personal para prevenir, detectar y contener cualquier vulneración de seguridad.

Un programa de formación y concienciación sobre seguridad comunica las políticas de seguridad a los empleados que desarrollan o respaldan el software Clarity LIMS. Un sistema de formación automatizado garantiza que todos los empleados necesarios reciban esta formación.

Todos los empleados que prestan soporte al software Clarity LIMS deben someterse a una formación anual sobre cómo gestionar los datos de los clientes. El acceso a los sistemas del cliente se concede por empleado. La descarga de datos está restringida y toda la actividad se registra y documenta en un sistema automatizado. Cuando los empleados que prestan soporte al software Clarity LIMS abandonan la empresa, se revoca su acceso a todos los sistemas del cliente y a los sistemas internos de Illumina. Se requisan todos los equipos y credenciales entregados al empleado.

Medidas relacionadas con las instalaciones

ISO/IEC 27001:2013 e ISO/IEC 27701:2019 para la nube de Clarity LIMS

La ISO 27001:2013 es un sistema de gestión de la seguridad de la información (ISMS, Information Security Management System) que busca colocar toda la gestión de la seguridad de la información bajo el control de la gestión, garantizando que los procesos y las políticas se desplieguen y apliquen de forma coherente y fiable. La norma establece cómo se almacenan y gestionan los datos y cómo se eliminan los activos de información. La ISO/IEC 27701:2019 es una norma de sistema de gestión de privacidad de la información (PIMS, Privacy Information Management System) que certifica que se implementan requisitos de privacidad de datos sólidos para garantizar que los datos se almacenen y mantengan de forma privada y conforme a la normativa. Las políticas en vigor para la conformidad con las normas ISO/IEC 27001:2013 e ISO/IEC 27701:2019 también establecen normas para el control del acceso, la gestión de contraseñas y la seguridad de la red.

Certificación ISO de Illumina

HIPAA

Nuestras instalaciones en las que se procesa la PHI cumplen con la HIPAA y con las mejores prácticas del sector. A continuación, se exponen ejemplos de las mejores prácticas que seguimos:

- Los edificios cuentan con vigilancia las 24 horas y el acceso a los mismos es mediante tarjetas identificativas.
- Las oficinas disponen de un sistema de seguridad supervisado.
- Los ordenadores utilizados para acceder o almacenar la PHI están protegidos con contraseña y tienen activado el cifrado de disco completo.
- Cualquier acceso desde fuera de la oficina se realiza a través de una red privada virtual (VPN, Virtual Private Network) segura.

Desarrollo de Clarity LIMS

El software Clarity LIMS se ha desarrollado y probado para crear una experiencia del usuario sólida, utilizable y predecible. El proceso de desarrollo del software determina la priorización de las características, la funcionalidad y la corrección de errores en función de las necesidades del negocio y los comentarios del cliente. Utilizamos una metodología Agile para desarrollar el software Clarity LIMS. La implementación particular del manifiesto Agile es Scrum, que es un método ampliamente utilizado y aceptado para ejecutar el proceso de desarrollo.

Las principales funciones de Agile incluyen ciclos de desarrollo cortos llamados «sprints», la capacidad de cambiar y adaptarse a las necesidades técnicas y de comercialización y la revisión y mejora constantes del proceso. Una vez finalizados, al menos otros dos desarrolladores revisan todos los cambios del código, excepto en el caso de pequeños cambios de redacción. El proceso de revisión ayuda a los desarrolladores a identificar problemas en el código base o en el uso de patrones de código que no cumplen los estándares. Si un código no cumple las expectativas, se revisará tantas veces como sea necesario hasta que cumpla los estándares. La metodología Agile permite varios puntos de control diseñados para ofrecer un sistema que cumpla o supere las expectativas del cliente. Esta y otras medidas de garantía de calidad, como la comprobación automatizada del código, garantizan que los sistemas entregados sean adecuados para su fin previsto y que los procesos utilizados sean correctos y adecuados.

Implementación y actualizaciones de la nube de Clarity LIMS

Ocasionalmente, Illumina publicará parches de seguridad y del sistema operativo (SO), correcciones de errores y otras versiones. Cuando se publiquen las versiones de parches de seguridad y Clarity LIMS, Illumina actualizará las instancias de Clarity LIMS correspondientes durante los periodos programados regularmente. Como parte de nuestras actividades de aplicación de parches, se puede actualizar lo siguiente:

- Parches del SO subyacente
- Software incluido subyacente o parches de Clarity LIMS
- Herramientas de Illumina, incluidos antivirus, registro, detección de intrusiones, copias de seguridad, etc.
- Componentes adicionales del sistema que no impiden la funcionalidad estándar de Clarity LIMS para la versión implementada

En el caso de las versiones menores y mayores, el personal de Illumina coordinará el tiempo de actualización con los clientes y proporcionará notificaciones de fin de vida útil, alojamiento y asistencia técnica para las versiones anteriores. Illumina normalmente aplicará versiones de parches a todas las versiones alojadas correspondientes durante los periodos programados regularmente, a menos que la seguridad u otros requisitos requieran una respuesta más rápida. Al final del alojamiento, Illumina puede actualizar las versiones anteriores que aún no se han actualizado a la versión más reciente de Clarity LIMS.

Prácticas de seguridad en el software Clarity LIMS

El software Clarity LIMS incluye varias funciones y medidas para promover la seguridad y la privacidad de los datos de la PHI.

Control de acceso

El trabajo de laboratorio requiere personal con distintas habilidades que trabaje en diversas tareas. A fin de evitar errores, pérdida de datos o manipulaciones, el acceso al sistema está restringido en función de los roles que requieran acceso. El software Clarity LIMS incluye un control de acceso configurable, con la capacidad de asignar acceso de solo lectura mediante ajustes de permisos basados en roles (habilitados a partir de Clarity LIMS v6.1).

Los usuarios con roles de administrador pueden configurar el acceso de modo que los usuarios designados tengan acceso de solo lectura, pero no de escritura. El modo de solo lectura admite el acceso seguro a los datos para una amplia gama de casos de uso de los clientes, incluida la auditoría, la generación de informes y la formación.

Cifrado en reposo (aplicación en la nube)

Cuando los datos están en reposo, el software Clarity LIMS utiliza Advanced Encryption System (AES)-256 para protegerlos. AES-256 es un conocido sistema de cifrado que es fácil de usar para los desarrolladores, pero difícil de descifrar para los jáqueres debido a su larga clave de 256 caracteres. AES-256 se utiliza de forma fiable en los sectores financiero, gubernamental y sanitario de todo el mundo.

Cifrado en tránsito

A fin de proteger los datos en tránsito, el software Clarity LIMS utiliza Transport Layer Security (TLS) 1.2 o una versión posterior. TLS es una tecnología estándar y bien establecida para cifrar el enlace entre un servidor web y un navegador web. Al igual que Advanced Encryption Standard (AES)-256, TLS se utiliza de forma fiable en muchos sectores, incluida la atención sanitaria.

Registro de actividades

En cualquier laboratorio, la trazabilidad de las muestras es importante, pero lo es aún más cuando se trabaja en entornos regidos por la normativa. El software Clarity LIMS permite el cumplimiento normativo mediante la producción de un registro de auditoría de cualquier muestra del sistema.

Un registro de auditoría es un seguimiento detallado de la muestra y de todas las acciones realizadas en la muestra desde su creación en LIMS. Los laboratorios pueden utilizar el registro de auditoría producido en el software Clarity LIMS para informar de la generación de informes del sistema o para cumplir con los requisitos de auditoría. El registro de auditoría en el software Clarity LIMS detalla todos los eventos durante el tiempo de vida de una muestra:

- Fecha y hora de adquisición y carga de la muestra
- Usuarios del laboratorio responsables de cualquier acción realizada en la muestra
- Reactivos utilizados con la muestra

Autenticación

El software Clarity LIMS utiliza un proceso de autenticación de un solo factor. Los usuarios inician sesión a través de un portal web con sus credenciales. Las organizaciones pueden integrar su proceso de contraseñas corporativas de modo que los usuarios de Clarity LIMS puedan iniciar sesión con sus contraseñas corporativas y el proceso Lightweight Directory Access Protocol (LDAP). La integración con LDAP está disponible como parte del software Clarity LIMS Enterprise.

Gestión de sesiones

El software Clarity LIMS incluye una función de gestión de sesiones para cerrar la sesión de los usuarios automáticamente tras 30 minutos de inactividad. Los usuarios con privilegios de administrador pueden configurar la gestión de sesiones.

Prevención de las vulnerabilidades de la red y de las aplicaciones

Los controles de límites supervisan y regulan las comunicaciones, el límite externo de la red y los límites internos clave. Estos controles de límites emplean juegos de reglas, listas de control de acceso y configuraciones para imponer el flujo de información a servicios específicos del sistema de información. Las listas de control de acceso, o políticas de flujo de tráfico, se establecen en cada interfaz gestionada para regular el flujo de tráfico. Los controles adicionales incluyen:

- Rastreo periódico de la red
- Política contra el uso del correo electrónico para la entrega de datos, mitigando el riesgo de los archivos adjuntos que podrían contener malware
- Respuesta priorizada para problemas de seguridad críticos

Pruebas de intrusión de terceros

Las pruebas de intrusión de terceros simulan un ataque al despliegue de un sistema y son una buena forma de probar las defensas de forma activa. Illumina emplea a un tercero imparcial para llevar a cabo pruebas de intrusión en las instancias en la nube de Clarity LIMS. Una vez que el proveedor finaliza la prueba, Illumina recibe un informe completo que detalla los resultados. Illumina no publica los resultados de estas pruebas de intrusión.

Integridad de los datos*

La copia de seguridad de la base de datos del cliente se realiza hasta 24 veces al día para reducir el riesgo de pérdida de datos. Además, el sistema contiene un registro que proporciona una notificación cuando se alteran los datos. Si se detecta una alteración incorrecta, puede volver a una versión anterior con copia de seguridad.

Copias de seguridad de datos

La nube de Clarity LIMS se somete a un riguroso proceso de copia de seguridad para su protección contra la pérdida de datos o ante desastres. La copia de seguridad de los datos se realiza mediante un sistema automatizado. Se realiza una copia de seguridad de la base de datos y de los archivos de datos externos asociados, así como de la configuración adecuada del sistema. Las copias de seguridad se cifran en tránsito a un área de almacenamiento S3 a la que solo puede acceder el personal autorizado. Illumina conserva tres juegos de copias de seguridad desde el momento en que se crean:

- Copias de seguridad por hora conservadas durante 2 días
- Copias de seguridad diarias conservadas durante 32 días
- Copias de seguridad mensuales conservadas durante 400 días

Recuperación ante desastres

En caso de desastre, se creará y configurará un nuevo sistema en la nube y se restaurará una copia de seguridad. Una vez implementado el nuevo sistema, Illumina trabajará con los usuarios del sistema para probar y asegurarse de que todos los datos estén en su lugar.

Planificamos una prueba de recuperación ante desastres anual. A medida que se lanzan nuevas versiones del software, es posible que sea necesario cambiar la copia de seguridad y el plan de recuperación ante desastres. Cualquier cambio necesario se realizará en el sistema de copia de seguridad y recuperación antes de cargar en el sistema cualquier dato del cliente.

Compatibilidad con la HIPAA

El software Clarity LIMS se ha diseñado e implementado para ser compatible con la HIPAA. El Congreso de los Estados Unidos promulgó la HIPAA en 1996 y, a partir de entonces, el Department of Health and Human Services de los Estados Unidos implantó múltiples normativas de desarrollo de dicha ley.[2] Entre otras cosas, la HIPAA estableció normas nacionales para la seguridad y privacidad de la PHI. Las principales disposiciones de la HIPAA incluyen la regla de seguridad (Security Rule) y la regla de notificación de vulneraciones (Breach Notification Rule).

La regla de seguridad de la HIPAA impone varios requisitos para garantizar la seguridad y privacidad de la PHI. El software Clarity LIMS incluye, entre otros, los requisitos de control de seguridad (Tabla 1, Tabla 2).

RGPD

El RGPD no solo se aplica a las empresas establecidas en la UE. Las empresas establecidas fuera de la UE, pero que trabajan con personas de la UE, también pueden estar sujetas al RGPD.

Como responsables del tratamiento de datos, los clientes son, en última instancia, los responsables de evaluar la aplicabilidad del RGPD a sus operaciones de tratamiento y de garantizar que cuenten con prácticas que cumplan con el RGPD. Sin embargo, dado que el RGPD es relevante para muchos de nuestros clientes, Clarity LIMS sigue los principios del RGPD aplicables a los encargados del tratamiento de datos.

Responsabilidades compartidas

Illumina es responsable de proteger la infraestructura que pone en marcha todos los servicios ofrecidos en AWS Cloud. Esta infraestructura se compone del hardware, el software, las redes y las instalaciones que ejecutan los servicios de AWS Cloud. Parte de esta responsabilidad requiere que Illumina realice actualizaciones periódicas de parches de seguridad u otras actualizaciones para proteger el entorno frente a las amenazas emergentes y respaldar mejoras iterativas. Illumina proporciona estas actualizaciones durante los periodos semanales definidos en los Términos y condiciones del software Clarity LIMS. Los clientes que deban cumplir la HIPAA son responsables de garantizar que cuenten con un programa de cumplimiento de la HIPAA.

Controles de seguridad

El uso del software Clarity LIMS pone varias responsabilidades en manos del cliente. La evaluación de riesgos debe tener en cuenta el uso de soluciones de software como servicio (SaaS) y los resultados de estas evaluaciones deben reflejarse en una revisión de los controles de privacidad y seguridad de cada cliente.

* Las mitigaciones de integridad de datos, de copia de seguridad de datos y de recuperación ante desastres se realizan únicamente para el software en la nube Clarity LIMS.

Los clientes deben revisar sus políticas para reflejar el uso del software Clarity LIMS. Las instituciones deben establecer procesos y procedimientos para la aprobación del acceso e implementar revisiones periódicas del acceso que se haya concedido a todos los usuarios. Además, las estaciones de trabajo utilizadas para acceder al software Clarity LIMS deben tener instaladas protecciones adecuadas, como software antivirus, cortafuegos en el equipo principal y registro centralizado. Los planes de continuidad del negocio y de recuperación ante desastres deben actualizarse para tener en cuenta el uso del software Clarity LIMS.

Tabla 2: Controles de seguridad en el software Clarity LIMS

Controles administrativos
Políticas y procedimientos para prevenir, detectar, contener y corregir vulneraciones de seguridad
Responsable de seguridad a cargo del desarrollo y la implementación de controles dentro de la organización
Procedimientos para garantizar que el acceso a los datos de los miembros del personal sea adecuado y esté aprobado
Configuración de permisos de acceso de solo lectura
Procesos para autorizar el acceso a los datos del cliente
Miembros del personal formados en la HIPAA
Procesos para la notificación de incidencias
Evaluación rutinaria para determinar cómo los cambios en otros procedimientos o en el entorno pueden afectar potencialmente a la seguridad
Controles físicos
Implementación de controles de acceso a las instalaciones
Alojamiento del software Clarity LIMS en centros de datos seguros
Políticas relativas a la seguridad de las estaciones de trabajo
Controles técnicos
ID de usuario único para cada usuario
Autenticación del usuario mediante el software Clarity LIMS o el LDAP de un cliente
Cifrado de datos en tránsito y en reposo

Respuesta ante incidencias y notificación de vulneraciones

En virtud de la HIPAA, los Socios comerciales deben cumplir con un juego de normas y reglamentos en relación con las vulneraciones potenciales y reales. Si se ha producido un intento de vulneración, Illumina realizará una evaluación de riesgos para determinar si el intento constituye una vulneración real. En caso de que lo fuera, Illumina informará al cliente tan pronto como sea razonablemente posible, siempre que los intentos infructuosos, como pings y otros ataques de difusión a nuestro cortafuegos, escaneos de puertos, intentos infructuosos de inicio de sesión, ataques de denegación de servicio y cualquier combinación de los anteriores, no constituyan un intento de vulneración.

Cumplimiento normativo del laboratorio

El software Clarity LIMS incluye numerosas funciones para respaldar el cumplimiento de las normativas, los estándares y las acreditaciones aplicables a los laboratorios que realizan pruebas en muestras humanas, como CLIA, CAP e ISO 15189. Entre ellas, se incluyen las siguientes:

- Seguimiento de muestras e historiales de muestras completos para fines de auditoría
- Herramientas que ayudan a cumplir con los procedimientos operativos estándar
- Seguimiento de reactivos y lotes
- Interfaces basadas en roles que permiten el acceso solo a funciones autorizadas
- Características de seguridad, como se describen en esta nota técnica

Información adicional

Software Clarity LIMS

Bibliografía

1. Amazon Web Services. AWS Cloud Security. aws.amazon.com/security/. Fecha de consulta: 28 de enero de 2023.
2. US Department of Health & Human Services. Summary of the HIPAA Privacy Rule. hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Fecha de actualización: 26 de julio de 2013. Fecha de consulta: 28 de enero de 2023.
3. Centers for Medicare & Medicaid Services. cms.gov/. Fecha de consulta: 28 de enero de 2023.
4. Centers for Medicare & Medicaid Services. CLIA Regulations and Federal Register Documents. cms.gov/Regulations-and-Guidance/Legislation/CLIA/CLIA_Regulations_and_Federal_Register_Documents. Fecha de actualización: 1 de diciembre de 2021. Fecha de consulta: 28 de enero de 2023.
5. College of American Pathologists. Acreditación. cap.org/laboratory-improvement/accreditation. Fecha de consulta: 28 de enero de 2023.

illumina®

1 800 809 4566 (llamada gratuita, EE. UU.) | tel.: +1 858 202 4566
techsupport@illumina.com | www.illumina.com

M-GL-00704 ESP v3.0