TECHNISCHER HINWEIS

Clarity LIMS™ – Sicherheit, Datenschutz und Compliance

Funktionen und Verfahren zum Schutz Ihrer Daten

illumina®

Durchsetzen strenger Sicherheits- und Datenschutzpraktiken

Die Sicherheit geschützter Gesundheitsdaten (PHI, Protected Health Information) wie genomischer Daten ist im globalen Geschäftsbetrieb von Illumina von grundlegender Bedeutung. Die in der Datenschutzrichtlinie unseres Unternehmens formulierten Datenschutzverfahren entsprechen den wichtigsten in nationalen und globalen Datenschutzvorschriften festgelegten Normen, einschließlich des Health Insurance Portability and Accountability Act (HIPAA), der Datenschutz-Grundverordnung (DSGVO) und des California Consumer Privacy Act (CCPA). Wir verpflichten uns zu den folgenden Leitprinzipien:

- **Transparenz:** Wir kommunizieren unsere Datenschutzpraktiken klar und deutlich und geben an, wie wir personenbezogene Daten verwenden.
- **Verantwortungsbewusstes Handeln:** Wir schützen personenbezogene Daten, damit sie vertraulich und sicher bleiben.
- **Ethische Verwendung:** Wir erfassen und verwenden personenbezogene Daten nur auf rechtmäßige und transparente Weise für Zwecke, die unsere Mission zur Verbesserung der menschlichen Gesundheit durch die Erschließung des Genoms fördern.
- **Rechenschaftspflicht:** Wir verpflichten uns zur Einhaltung aller gesetzlichen Anforderungen und zur Förderung interner Praktiken, um die höchsten Standards für den Schutz personenbezogener Daten zu erreichen.

Sicherheitsframeworks

Strenge institutionelle Datenschutzpraktiken basieren auf einem erfolgreichen Datensicherheitsprogramm. Zwar kommen weltweit zahlreiche verschiedene Sicherheitsframeworks zum Einsatz, wir konzentrieren uns bei unseren Praktiken und diesem technischen Hinweis jedoch auf die am häufigsten verwendeten, darunter:

- HIPAA
- Internationale Organisation für Normung (ISO, International Organization for Standardization) 27001 (Sicherheit) und 27701 (Datenschutz)

Infrastruktur

Illumina nutzt für die Sicherheit von Clarity LIMS (Laboratory Information Management System) eigene Sicherheitsmaßnahmen und -verfahren. Daneben setzen wir auf einen umfassenden und bewährten Ansatz, der von Amazon Web Services (AWS) übernommen wurde (Abbildung 1).[1]

Sicherheit auf einen Blick

In Tabelle 1 finden Sie einen umfassenden Überblick über die in der Clarity LIMS-Software enthaltenen Sicherheitsmaßnahmen. Ausführliche Informationen finden Sie weiter unten in diesem technischen Hinweis.

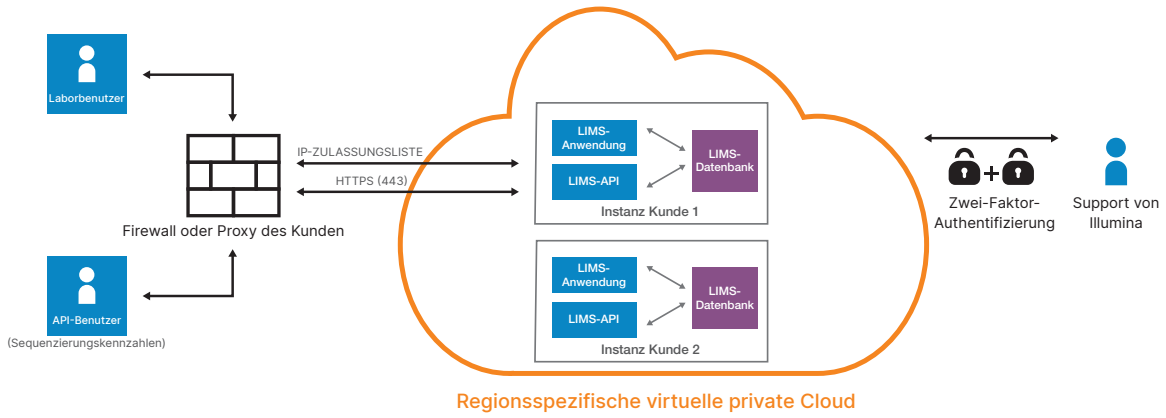

Abbildung 1: Die Sicherheitsinfrastruktur der Clarity LIMS-Software

Tabelle 1: Checkliste zu Sicherheit und Datenschutz für Clarity LIMS

Intern und verfahrenstechnisch			
Hintergrundprüfungen für Mitarbeiter	✓	Überwachung	✓
Sicherheitsrichtlinien	✓	Reaktion auf Vorfälle	✓
Zugriffskontrolle	✓	Schutz vor Malware	✓
Lesezugriff rollenspezifisch möglich	✓	Notfallwieder-herstellungspläne	✓
Sicherungen	✓		
Cloudanwendung			
Zugriffskontrolle	✓	Schutz vor Malware	✓
Verschlüsselung bei Speicherung	✓	Notfall-wiederherstellung	✓
Verschlüsselung bei Datenübermittlung	✓	Datensicherung	✓
Protokollierung von Aktivitäten	✓	Datenintegrität	✓
Penetrationstest durch Drittanbieter	✓	Codeprüfung/-test	✓
Rollenbasierte Zugriffskontrolle	✓	Netzwerk	✓
Kennwortkontrollen	✓	Netzwerk-segmentierung	✓
Sitzungsmanagement	✓		
Compliance und Nachweis – Version 5.4 und höher			
ISO/IEC 27001:2013 (für Cloudinstanzen)	✓	HIPAA (von Drittanbieter validiert)	✓
ISO/IEC 27701:2019 (für Cloudinstanzen, v6.1 und höher)	✓		

Sicherheitspraktiken für Mitarbeiter

Unsere Sicherheitspraktiken beginnen noch vor dem Onboarding neuer Mitarbeiter. Wir führen Hintergrundprüfungen aller Bewerber durch, sofern dies gesetzlich zulässig ist. Dokumentierte Richtlinien leiten das Personal bei der Verhinderung, Erkennung und Eindämmung von Sicherheitsverstößen an.

In einer Schulung zum Sicherheitsbewusstsein erhalten Mitarbeiter, die in der Entwicklung oder im Support der Clarity LIMS-Software tätig sind, eine Einweisung in die Sicherheitsrichtlinien. Mit einem automatisierten Schulungssystem wird sichergestellt, dass alle erforderlichen Mitarbeiter diese Schulung absolvieren.

Für alle Supportmitarbeiter für die Clarity LIMS-Software ist eine jährliche Schulung zum Umgang mit Kundendaten obligatorisch. Der Zugriff auf Kundensysteme wird für bestimmte Mitarbeiter individuell gewährt. Das Herunterladen von Daten ist eingeschränkt und alle Aktivitäten werden in einem automatisierten System protokolliert und dokumentiert. Wenn Supportmitarbeiter für die Clarity LIMS-Software das Unternehmen verlassen, wird ihnen der Zugriff auf alle Kundensysteme und internen Illumina-Systeme entzogen. Alle Geräte und Ausweise, die dem jeweiligen Mitarbeiter zur Verfügung gestellt wurden, werden eingezogen.

Einrichtungsbezogene Maßnahmen

ISO/IEC 27001:2013 und ISO/IEC 27701:2019 für Clarity LIMS-Cloudinstanzen

ISO 27001:2013 ist eine Norm für Informations-sicherheitsmanagementsysteme (ISMS), bei der das gesamte Informationssicherheitsmanagement in die Zuständigkeit des Managements fällt. So wird sichergestellt, dass Prozesse und Richtlinien konsistent und zuverlässig eingeführt und durchgesetzt werden. Die Norm gibt vor, wie Daten gespeichert und verwaltet werden und wie Datenbestände entsorgt werden. ISO/IEC 27701:2019 ist eine Norm für Datenschutzinformationsmanagementsysteme (PIMS, Privacy Information Management System), mit der die Implementierung strenger Datenschutzanforderungen zertifiziert wird. So wird sichergestellt, dass Daten vertraulich und gemäß den entsprechenden Bestimmungen gespeichert und aufbewahrt werden. Durch die in ISO/IEC 27001:2013 und ISO/IEC 27701:2019 verankerten Richtlinien werden auch Standards für die Zugriffskontrolle, das Kennwortmanagement und die Netzwerksicherheit festgelegt.

ISO-Zertifizierung für Illumina

HIPAA

Unsere Einrichtungen, in denen PHI verarbeitet werden, entsprechen HIPAA und in der Branche bewährten Best Practices. Beispiele für Best Practices, die wir befolgen:

- Gebäude werden rund um die Uhr überwacht und sind nur mit Zugangskarten zugänglich.
- Büros verfügen über ein überwachtes Sicherheitssystem.
- Computer, die für den Zugriff auf oder die Speicherung von PHI verwendet werden, sind kennwortgeschützt und verfügen über eine aktivierte Festplattenverschlüsselung.
- Jeder Zugriff von außerhalb des Büros erfolgt über ein sicheres VPN (Virtual Private Network).

Clarity LIMS-Entwicklung

Die Clarity LIMS-Software wurde entwickelt und getestet, um Anwendern eine stabile, praktische und zuverlässige Erfahrung zu bieten. Im Softwareentwicklungsprozess werden Eigenschaften, Funktionen und Fehlerbehebungen auf Grundlage von Geschäftsanforderungen und Kundeninformationen priorisiert. Die Clarity LIMS-Software wird unter Einsatz der Agile-Methode entwickelt. Die spezifische Implementierung des Agile-Manifests ist Scrum, eine weit verbreitete und akzeptierte Methode zur Verwaltung des Entwicklungsprozesses.

Zu den wichtigsten Merkmalen von Agile gehören kurze Entwicklungszyklen, die als Sprints bezeichnet werden, die Fähigkeit, Marketing- und technische Anforderungen zu ändern und anzupassen, sowie die ständige Überprüfung und Verbesserung des Prozesses. Nach Abschluss werden alle Codeänderungen von mindestens zwei anderen Entwicklern überprüft, außer bei geringfügigen Änderungen. Der Überprüfungsprozess hilft Entwicklern, Probleme in der Codebasis oder die Verwendung von Codemustern, die nicht den Standards entsprechen, zu identifizieren. Code, der nicht den Standards entspricht, wird überarbeitet und überprüft, bis er die Standards erfüllt. Die Agile-Methode ermöglicht mehrere Kontrollpunkte, um ein System bereitzustellen, das die Kundenerwartungen erfüllt oder übertrifft. Mit diesen und anderen Qualitätssicherungsmaßnahmen, wie z. B. der automatischen Codeprüfung, wird sichergestellt, dass die bereitgestellten Systeme für den jeweiligen Zweck tauglich sind und dass die verwendeten Prozesse korrekt und geeignet sind.

Implementierung und Updates der Clarity LIMS-Cloudinstanz

Von Zeit zu Zeit stellt Illumina Sicherheits- und Betriebssystem-Patches, Fehlerbehebungen und andere Veröffentlichungen bereit. Mit der Veröffentlichung von Sicherheits- und Clarity LIMS-Patchversionen aktualisiert Illumina die entsprechenden Clarity LIMS-Instanzen in regulär geplanten Zeitfenstern. Im Rahmen der Patching-Maßnahmen kann Folgendes aktualisiert werden:

- Patches für das zugrunde liegende Betriebssystem
- Patches für die zugrunde liegende Software oder Clarity LIMS
- Illumina-Tools, einschließlich Virenschutz, Protokollierung, Erkennung von unberechtigtem Zugriff, Sicherungen usw.
- Zusätzliche Komponenten des Systems, die die standardmäßige Clarity LIMS-Funktionalität für die bereitgestellte Version nicht beeinträchtigen

Bei Neben- und Hauptversionen koordinieren Illumina-Mitarbeiter den Zeitpunkt des Upgrades mit den Kunden und senden für ältere Versionen Benachrichtigungen über das Ende von Lebensdauer, Hosting und Support. Illumina wendet in der Regel Patchversionen auf alle anwendbaren gehosteten Versionen während regulär geplanter Zeitfenster an, es sei denn, sicherheitsbezogene oder sonstige Anforderungen verlangen eine schnellere Reaktion. Zum Ende des Hostings werden ältere Versionen, die noch nicht auf die neueste Clarity LIMS-Version aktualisiert wurden, von Illumina möglicherweise aktualisiert.

Sicherheitspraktiken in der Clarity LIMS-Software

Die Clarity LIMS-Software umfasst mehrere Funktionen und Maßnahmen zur Förderung der Sicherheit und des Datenschutzes von PHI-Daten.

Zugriffskontrolle

Für Laborarbeit werden Mitarbeiter mit unterschiedlichen Fähigkeiten für eine Vielzahl von Aufgaben benötigt. Um Fehler, Datenverlust oder Manipulationen zu verhindern, ist der Systemzugriff auf die für die jeweilige Rolle erforderlichen Funktionen beschränkt. Die Clarity LIMS-Software umfasst eine konfigurierbare Zugriffskontrolle, mit der Lesezugriff über rollenbasierte Berechtigungseinstellungen (ab Clarity LIMS v6.1 aktiviert) zugewiesen werden kann.

Benutzer mit Administratorrollen können den Zugriff so konfigurieren, dass bestimmte Benutzer über Lese-, jedoch nicht über Schreibzugriff verfügen. Der schreibgeschützte Modus unterstützt den sicheren Datenzugriff für bestimmte Kundenanwendungsfälle wie Auditing, Befunderstellung und Schulung.

Verschlüsselung bei Speicherung (Cloudanwendung)

Beim Speichern der Daten verwendet die Clarity LIMS-Software zum Schutz der Daten AES-256 (Advanced Encryption Standard). AES-256 ist ein bekanntes Verschlüsselungssystem, das für Entwickler einfach zu verwenden, aufgrund seines langen 256-stelligen Schlüssels für Hacker jedoch schwierig zu überwinden ist. AES-256 wird weltweit zuverlässig in der Finanz- und Gesundheitsbranche sowie in Behörden eingesetzt.

Verschlüsselung bei Datenübermittlung

Bei der Übermittlung verwendet die Clarity LIMS-Software zum Schutz der Daten TLS 1.2 (Transport Layer Security) oder höher. TLS ist eine bewährte Standardtechnologie zum Verschlüsseln der Verbindung zwischen einem Webserver und einem Webbrowser. Wie AES-256 (Advanced Encryption Standard) wird TLS in vielen Branchen, beispielsweise der Gesundheitsversorgung, zuverlässig eingesetzt.

Protokollierung von Aktivitäten

Die Rückverfolgbarkeit von Proben ist in jedem Labor wichtig. Bei der Arbeit in regulierten Umgebungen gewinnt sie jedoch noch an Bedeutung. Die Clarity LIMS-Software unterstützt die Compliance, indem für jede Probe ein Prüfpfad im System erstellt wird.

Ein Prüfpfad ist eine detaillierte Darstellung der Probe und aller Aktivitäten, die seit der Erstellung im LIMS an ihr durchgeführt wurden. Labore können den in der Clarity LIMS-Software erstellten Prüfpfad für die Systemberichterstellung oder die Erfüllung der Prüfungsanforderungen nutzen. Im Prüfpfad der Clarity LIMS-Software werden alle Ereignisse während der Lebensdauer einer Probe aufgeführt:

- Datum und Uhrzeit der Probenerfassung und des Hochladens
- Laboranwender, die für die an der Probe durchgeführten Aktivitäten verantwortlich sind
- Mit der Probe verwendete Reagenzien

Authentifizierung

Die Clarity LIMS-Software verwendet einen Ein-Faktor-Authentifizierungsprozess. Benutzer melden sich über ein Webportal mit ihren Anmeldedaten an. Unternehmen können ihren internen Kennwortprozess integrieren, sodass sich Clarity LIMS-Benutzer mit ihrem jeweiligen Unternehmenskennwort und über den LDAP-Prozess (Lightweight Directory Access Protocol) anmelden können. Die LDAP-Integration ist als Teil der Clarity LIMS Enterprise-Software verfügbar.

Sitzungsmanagement

Clarity LIMS umfasst eine Sitzungsmanagement-funktion, mit der Benutzer nach einer Inaktivität von 30 Minuten automatisch abgemeldet werden. Das Sitzungsmanagement kann von Benutzern mit Administratorrechten konfiguriert werden.

Verhindern von Risiken in Netzwerk und Anwendungen

Die Kommunikation sowie die äußere Netzwerkgrenze und wichtige interne Netzwerkgrenzen werden durch entsprechende Kontrollen überwacht und reguliert. Diese Kontrollen steuern den Datenfluss zu bestimmten Systemdiensten anhand von Regelsätzen, Zugriffskontrolllisten und Konfigurationen. Auf jeder verwalteten Schnittstelle werden Zugriffskontrolllisten oder Richtlinien erstellt, die den Datenverkehr regulieren. Zu den weiteren Kontrollen zählen:

- Regelmäßiges Scannen des Netzwerks
- Richtlinie gegen die Verwendung von E-Mails für den Datenversand, um das Risiko von Anlagen mit Malware zu minimieren
- Priorisierte Reaktion auf kritische Sicherheitsprobleme

Penetrationstests durch Drittanbieter

Bei Penetrationstests durch Drittanbieter wird ein Angriff auf ein System simuliert, um Abwehrmaßnahmen aktiv zu testen. Illumina beauftragt einen unbefangenen Drittanbieter mit der Durchführung von Penetrationstests für Clarity LIMS-Cloudinstanzen. Nachdem der Anbieter den Test abgeschlossen hat, erhält Illumina einen umfassenden Bericht mit den Ergebnissen. Die Ergebnisse dieser Penetrationstests werden von Illumina nicht veröffentlicht.

Datenintegrität*

Die Sicherung der Kundendatenbank erfolgt bis zu 24-mal täglich, um das Risiko von Datenverlust zu verringern. Darüber hinaus umfasst das System eine Protokollierung, die Benachrichtigungen bei der Änderung von Daten ausgibt. Wenn eine unsachgemäße Änderung festgestellt wird, kann eine zuvor gesicherte Version wiederhergestellt werden.

Datensicherungen

Zum Schutz vor Datenverlust bzw. für Notfallmaßnahmen werden Clarity LIMS-Cloudinstanzen einem strengen Sicherungsprozess unterzogen. Die Datensicherung erfolgt über ein automatisiertes System. Sowohl die Datenbank als auch die zugehörigen externen Datendateien und die entsprechende Systemkonfiguration werden gesichert. Sicherungen werden bei Übertragung in einen S3-Speicherbereich verschlüsselt, der nur autorisiertem Personal zugänglich ist. Illumina speichert drei Sicherungssätze für folgende Zeiträume (ab dem Zeitpunkt der Erstellung):

- Stündliche Sicherung, Aufbewahrungdauer: 2 Tage
- Tägliche Sicherung, Aufbewahrungsdauer: 32 Tage
- Monatliche Sicherung, Aufbewahrungsdauer: 400 Tage

Notfallwiederherstellung

Bei einem Notfall wird ein neues Cloudsystem erstellt und konfiguriert und eine Sicherung wird wiederhergestellt. Nach der Implementierung des neuen Systems überprüft Illumina gemeinsam mit Systemanwendern, ob alle Daten vorhanden sind.

Ein Notfallwiederherstellungstest wird jährlich durchgeführt. Wenn neue Versionen der Software veröffentlicht werden, muss der Sicherungs- und Notfallwiederherstellungsplan möglicherweise geändert werden. Alle erforderlichen Änderungen am Sicherungs- und Wiederherstellungssystem werden vor dem Go-Live des Systems mit allen Kundendaten vorgenommen.

Unterstützung für HIPAA

Die Clarity LIMS-Software wurde für die Unterstützung von HIPAA entwickelt und implementiert. HIPAA wurde 1996 vom US-Kongress verabschiedet. Danach wurden vom US-Gesundheitsministerium mehrere Vorschriften eingeführt, um das Gesetz in die Praxis umzusetzen.[2]

Durch HIPAA wurden unter anderem nationale Standards für die Sicherheit und den Datenschutz von PHI festgelegt. Zu den wichtigsten HIPAA-Bestimmungen zählen die Security Rule (Sicherheitsvorschrift) und die Breach Notification Rule (Vorschrift zur Meldung von Verstößen).

Mit der HIPAA Security Rule werden mehrere Anforderungen definiert, um die Sicherheit und den Datenschutz von PHI zu gewährleisten. Die Clarity LIMS-Software umfasst u. a. Anforderungen für Sicherheitsmaßnahmen (Tabelle 1, Tabelle 2).

DSGVO

Die DSGVO gilt nicht nur für in der EU ansässige Unternehmen. Unternehmen, die außerhalb der EU ansässig sind, jedoch Kunden in der EU haben, unterliegen möglicherweise auch der DSGVO.

Als Datenverantwortliche sind Kunden letztendlich dafür verantwortlich, die Anwendbarkeit der DSGVO auf ihre Verarbeitungsvorgänge zu bewerten und sicherzustellen, dass sie DSGVO-konforme Verfahren anwenden. Da die DSGVO jedoch für viele unserer Kunden relevant ist, befolgt Clarity LIMS die für Datenverarbeiter geltenden DSGVO-Prinzipien.

Gemeinsame Verantwortlichkeiten

Illumina ist für den Schutz der Infrastruktur verantwortlich, auf der alle in der AWS Cloud angebotenen Dienste ausgeführt werden. Diese Infrastruktur besteht aus Hardware, Software, Netzwerk und Einrichtungen, die AWS Cloud-Dienste ausführen. Im Rahmen dieser Verantwortung führt Illumina regelmäßig Sicherheitspatch-Updates oder andere Updates durch, um die Umgebung vor aufkommenden Bedrohungen zu schützen und iterative Verbesserungen zu unterstützen. Illumina stellt diese Updates in wöchentlichen Zeitfenstern bereit, die in den allgemeinen Geschäftsbedingungen der Clarity LIMS-Software definiert sind. Kunden, die an HIPAA gebunden sind, müssen sicherstellen, dass sie über ein Programm zur Sicherstellung der HIPAA-Compliance verfügen.

Sicherheitsmaßnahmen

Mit der Verwendung der Clarity LIMS-Software werden dem Kunden verschiedene Verantwortlichkeiten übertragen. Bei der Risikobewertung muss die Verwendung von SaaS-Lösungen (Software as a Service) berücksichtigt werden und die Ergebnisse dieser Bewertung sollten in eine Überprüfung der Datenschutz- und Sicherheitsmaßnahmen der einzelnen Kunden einfließen.

* Maßnahmen zur Datenintegrität, Datensicherung und Notfallwiederherstellung werden nur für die Clarity LIMS-Cloudsoftware durchgeführt.

Kunden sollten ihre Richtlinien hinsichtlich der Verwendung der Clarity LIMS-Software überprüfen. Einrichtungen sollten Prozesse und Verfahren für die Zugriffsgenehmigung festlegen und regelmäßige Überprüfungen des Zugriffs, der allen Benutzern gewährt wurde, einführen. Darüber hinaus müssen auf Workstations, die für den Zugriff auf die Clarity LIMS-Software verwendet werden, geeignete Schutzfunktionen installiert sein, z. B. Virenschutzsoftware, hostbasierte Firewalls und zentralisierte Protokollierung. Pläne für die Sicherstellung der Geschäftskontinuität und die Notfallwiederherstellung sollten aktualisiert werden, um die Verwendung der Clarity LIMS-Software zu berücksichtigen.

Tabelle 2: Sicherheitsmaßnahmen in der Clarity LIMS-Software

Administrative Maßnahmen
Richtlinien und Verfahren zur Verhinderung, Erkennung, Eindämmung und Korrektur von Sicherheitsverstößen
Sicherheitsbeauftragter, der für die Entwicklung und Implementierung von Maßnahmen innerhalb des Unternehmens verantwortlich ist
Verfahren zur Sicherstellung, dass der Mitarbeiterzugriff auf Daten angemessen ist und genehmigt wurde
Berechtigungseinstellung für Lesezugriff
Prozesse zur Autorisierung des Zugriffs auf Kundendaten
Für HIPAA geschulte Mitarbeiter
Prozesse zur Meldung von Vorfällen
Routinemäßige Bewertung, um festzustellen, wie sich Änderungen an anderen Verfahren oder der Umgebung auf die Sicherheit auswirken können
Physische Maßnahmen
Implementierte Zugangskontrollen für die Einrichtung
Hosting der Clarity LIMS-Software in sicheren Rechenzentren
Richtlinien zur Sicherheit der Workstations
Technische Maßnahmen
Eindeutige Benutzer-ID für jeden Benutzer
Benutzerauthentifizierung durch Clarity LIMS-Software oder LDAP des Kunden
Verschlüsselung von Daten bei Übertragung und Speicherung

Vorfallreaktion und Meldung von Verstößen

Geschäftspartner müssen gemäß HIPAA eine Reihe von Regeln und Vorschriften bezüglich potenzieller und tatsächlicher Verstöße einhalten. Im Falle eines versuchten Verstoßes führt Illumina eine Risikobewertung durch, um festzustellen, ob der Versuch einen tatsächlichen Verstoß darstellt. In diesem Fall benachrichtigt Illumina den Kunden so schnell wie möglich, vorausgesetzt, dass erfolglose Versuche wie Pings und andere Broadcast-Angriffe auf unsere Firewall, Port-Scans, erfolglose Anmeldeversuche, Denial-of-Service-Angriffe und beliebige Kombinationen der oben genannten Angriffe keinen versuchten Verstoß darstellen.

Labor-Compliance

Die Clarity LIMS-Software umfasst zahlreiche Funktionen zur Unterstützung der Compliance mit Vorschriften, Normen und Zulassungen, die für Labore gelten, in denen Tests an menschlichen Proben durchgeführt werden, z. B. CLIA, CAP und ISO 15189. Dazu zählen:

- Probenverfolgung und vollständige Probenverläufe für Prüfungszwecke
- Tools zur Unterstützung der Einhaltung von Standardbetriebsverfahren
- Reagenzien- und Chargenverfolgung
- Rollenbasierte Benutzeroberflächen, die den Zugriff auf autorisierte Funktionen beschränken
- Sicherheitsfunktionen, wie in diesem technischen Hinweis beschrieben

Weitere Informationen

Clarity LIMS-Software

Quellen

1. Amazon Web Services. AWS Cloud Security. aws.amazon.com/security/. Aufgerufen am 28. Januar 2023.
2. US Department of Health & Human Services. Summary of the HIPAA Privacy Rule. hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Aktualisiert am 26. Juli 2013. Aufgerufen am 28. Januar 2023.
3. Centers for Medicare & Medicaid Services. cms.gov/. Aufgerufen am 28. Januar 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. Aktualisiert am 1. Dezember 2021. Aufgerufen am 28. Januar 2023.
5. College of American Pathologists. Accreditation. cap.org/laboratory-improvement/accreditation. Aufgerufen am 28. Januar 2023.

illumina®

1 800 8094566 (USA, gebührenfrei) | +1 858 2024566 (Tel. außerhalb der USA)
techsupport@illumina.com | www.illumina.com

M-GL-00704 DEU v3.0