NOTA TECNICA

Sicurezza, privacy e conformità di Clarity LIMS™

Le funzionalità e l'approccio che contribuiscono a proteggere i dati

illumina®

Introduzione di solide pratiche di sicurezza e privacy

In base alle procedure operative aziendali globali di Illumina, è fondamentale salvaguardare la privacy delle informazioni protette sulla salute del paziente (PHI, Protected Health Information), inclusi i dati genomici. Il nostro approccio alla protezione dei dati e alla privacy, come descritto nella nostra Politica sulla privacy aziendale, è in linea con gli standard chiave stabiliti dalle normative nazionali e globali sulla privacy dei dati, tra cui l'Health Insurance Portability and Accountability Act (HIPAA), il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) e il California Consumer Privacy Act (CCPA). Ci impegniamo a rispettare i seguenti principi guida:

- **Trasparenza**. Comunichiamo chiaramente le nostre pratiche sulla privacy e il modo in cui utilizziamo i dati personali
- **Gestione responsabile**. Proteggiamo i dati personali per mantenerli riservati e sicuri
- **Uso etico**. Raccogliamo e utilizziamo i dati personali solo in modo lecito e trasparente per scopi che promuovono la nostra mission di migliorare la salute umana sfruttando le potenzialità del genoma
- **Responsabilità**. Ci impegniamo a rispettare tutti i requisiti legali e a promuovere le pratiche interne per raggiungere gli standard più elevati per la privacy dei dati personali

Framework di sicurezza

Le solide pratiche istituzionali sulla privacy si basano su un proficuo programma di sicurezza delle informazioni. Sebbene siano in atto vari framework di sicurezza a livello globale, le nostre pratiche e questa nota tecnica si concentrano sui framework più comuni, tra cui:

- HIPAA
- International Organization for Standardization (ISO) 27001 (sicurezza) e 27701 (privacy)

Infrastruttura

Illumina applica controlli e procedure interni per la sicurezza di Clarity LIMS (Laboratory Information Management System, sistema di gestione delle informazioni di laboratorio), insieme a un approccio completo e ben collaudato ereditato da Amazon Web Services (AWS) (Figura 1).[1]

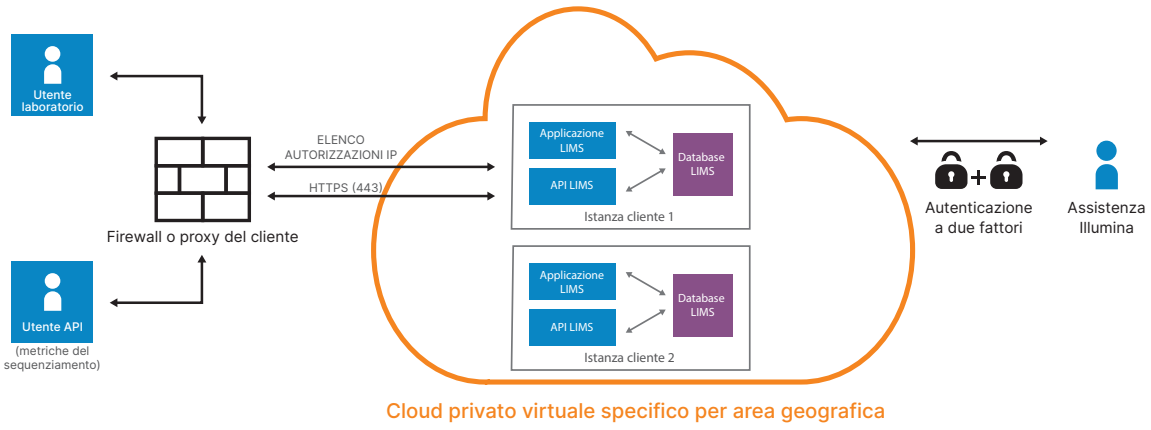

Figura 1: infrastruttura di sicurezza del software Clarity LIMS.

Panoramica sulle procedure di sicurezza

Nella Tabella 1 è fornita una panoramica di alto livello dei controlli di sicurezza integrati nel software Clarity LIMS. Le informazioni dettagliate sono fornite nella parte restante di questa nota tecnica.

Tabella 1. Lista di controllo per la sicurezza e la privacy di Clarity LIMS

Controlli interni e procedurali			
Verifiche dei precedenti personali dei dipendenti	✓	Monitoraggio	✓
Politiche di sicurezza	✓	Risposta agli incidenti	✓
Controllo degli accessi	✓	Anti-malware	✓
Accesso in sola lettura assegnabile al ruolo	✓	Piani di ripristino di emergenza	✓
Backup	✓		
Applicazione cloud			
Controllo degli accessi	✓	Anti-malware	✓
Crittografia a riposo	✓	Ripristino di emergenza	✓
Crittografia in transito	✓	Backup dei dati	✓
Registrazione delle attività	✓	Integrità dei dati	✓
Penetration test di terze parti	✓	Revisione/test del codice	✓
Controllo degli accessi basato sui ruoli	✓	Rete	✓
Controlli delle password	✓	Segmentazione della rete	✓
Gestione delle sessioni	✓		
Conformità e attestazione - Versione 5.4 e successive			
ISO/IEC 27001:2013 (per istanze cloud)	✓	HIPAA (convalidato da terze parti)	✓
ISO/IEC 27701:2019 (per istanze cloud, v6.1 e successive)	✓		

Pratiche di sicurezza per i dipendenti

Le nostre pratiche di sicurezza iniziano prima dell'arrivo di nuovi dipendenti. Eseguiamo controlli sui precedenti personali di tutti i candidati al ruolo di dipendenti, laddove consentito dalle leggi vigenti. Le politiche documentate rappresentano un riferimento per il personale nella prevenzione, nel rilevamento e nel contenimento di eventuali violazioni della sicurezza.

Un programma di sensibilizzazione e formazione sulla sicurezza descrive le politiche di sicurezza ai dipendenti che sviluppano o forniscono assistenza per il software Clarity LIMS. Un sistema di formazione automatizzato assicura che tutti i dipendenti a cui è richiesto completino questa formazione.

Tutti i dipendenti che forniscono assistenza per il software Clarity LIMS devono seguire una formazione annuale su come gestire i dati dei clienti. L'accesso ai sistemi dei clienti viene concesso a ogni dipendente. Il download dei dati è limitato e tutte le attività vengono registrate e documentate in un sistema automatizzato. Quando i dipendenti che utilizzano il software Clarity LIMS lasciano l'azienda, il loro accesso a tutti i sistemi dei clienti e ai sistemi Illumina interni viene revocato. Tutte le apparecchiature e i badge forniti al dipendente vengono ceduti.

Misure relative alla struttura

ISO/IEC 27001:2013 e ISO/IEC 27701:2019 per il cloud di Clarity LIMS

ISO 27001:2013 è un sistema di gestione della sicurezza delle informazioni (ISMS, Information Security Management System) il cui scopo è porre tutta la gestione della sicurezza delle informazioni sotto il controllo della direzione, garantendo che i processi e le politiche siano implementati e applicati in modo coerente e affidabile. Lo standard stabilisce il modo in cui i dati vengono archiviati e gestiti e il modo in cui le risorse informative vengono smaltite. ISO/IEC 27701:2019 è uno standard del sistema di gestione delle informazioni sulla privacy (PIMS, Privacy Information Management System) che certifica l'implementazione di solidi requisiti sulla privacy dei dati per garantire che i dati siano archiviati e conservati in modo privato e conforme. Le politiche in vigore per gli standard ISO/IEC 27001:2013 e ISO/IEC 27701:2019 stabiliscono anche gli standard per il controllo degli accessi, la gestione delle password e la sicurezza della rete.

Certificazione ISO di Illumina

HIPAA

Le nostre strutture in cui vengono elaborate le PHI sono conformi all'HIPAA e alle best practice del settore. Ad esempio, ci atteniamo alle seguenti best practice:

- Gli edifici sono monitorati 24 ore su 24 e sono accessibili con chiave elettronica
- Gli uffici dispongono di un sistema di sicurezza monitorato
- I computer utilizzati per accedere o archiviare le PHI sono protetti da password e dalla crittografia completa del disco
- Qualsiasi accesso dall'esterno dell'ufficio avviene tramite una rete privata virtuale (VPN, Virtual Private Network) sicura

Sviluppo di Clarity LIMS

Il software Clarity LIMS è stato sviluppato e testato per creare un'esperienza stabile, intuitiva e prevedibile per gli utenti. Lo sviluppo del software determina la priorità delle funzionalità, delle funzioni e delle correzioni dei bug da implementare, in base alle esigenze aziendali e all'input del cliente. Utilizziamo una metodologia Agile per sviluppare il software Clarity LIMS. La particolare implementazione del programma Agile è Scrum, un metodo ampiamente utilizzato e accettato per eseguire il processo di sviluppo.

Le principali funzioni di Agile includono brevi cicli di sviluppo denominati sprint, la capacità di cambiare e adattarsi alle esigenze tecniche e di marketing e la revisione e il miglioramento costanti del processo. Al termine, tutte le modifiche al codice vengono esaminate da almeno altri due sviluppatori, tranne nel caso di piccole modifiche alla formulazione. Il processo di revisione aiuta gli sviluppatori a identificare i problemi nella base di codice o l'uso di modelli di codice non conformi agli standard. Il codice non conforme agli standard sarà rivisto ed esaminato fino a quando non soddisfa questi ultimi. La metodologia Agile offre più punti di controllo progettati per fornire un sistema che soddisfi o superi le aspettative dei clienti. Questa e altre misure di garanzia della qualità, come il controllo automatico del codice, assicurano che i sistemi forniti siano adatti al loro scopo e che i processi utilizzati siano corretti e adeguati.

Implementazione e aggiornamenti del cloud di Clarity LIMS

Di tanto in tanto, Illumina rilascerà patch di sicurezza e del sistema operativo (SO), correzioni di bug e altre versioni. Quando vengono rilasciate le versioni delle patch di sicurezza e di Clarity LIMS, Illumina aggiorna le istanze Clarity LIMS applicabili durante le finestre regolarmente programmate. Per quanto riguarda le patch che rilasciamo, ecco gli aspetti che potrebbero subire aggiornamenti:

- Patch del sistema operativo di base
- Patch del software incluso di base o del Clarity LIMS
- Strumenti Illumina, inclusi antivirus, registrazione, rilevamento di intrusioni, backup, ecc.
- Componenti aggiuntivi del sistema che non interrompono la funzionalità standard di Clarity LIMS per la versione utilizzata

Per le versioni secondarie e principali, il personale Illumina coordinerà le tempistiche di aggiornamento con i clienti e invierà notifiche di fine vita, hosting e assistenza per le versioni precedenti. In genere, Illumina applicherà le versioni delle patch a tutte le versioni ospitate applicabili durante le finestre regolarmente programmate, a meno che la sicurezza o altri requisiti non richiedano una risposta più rapida. Al termine dell'hosting, Illumina potrebbe aggiornare le versioni precedenti non ancora aggiornate alla versione più recente di Clarity LIMS.

Pratiche di sicurezza nel software Clarity LIMS

Il software Clarity LIMS include diverse funzionalità e misure per promuovere la sicurezza e la privacy dei dati PHI.

Controllo degli accessi

Il lavoro di laboratorio richiede personale con competenze diversificate, in grado di occuparsi di un'ampia gamma di attività. Per evitare errori, perdita di dati o manomissione, l'accesso al sistema prevede limitazioni in base ai ruoli che necessitano dell'accesso. Il software Clarity LIMS include il controllo degli accessi configurabile, con la possibilità di assegnare l'accesso in sola lettura tramite le impostazioni delle autorizzazioni basate sul ruolo (disponibili a partire da Clarity LIMS v6.1).

Gli utenti amministratori possono configurare l'accesso in modo che gli utenti designati abbiano accesso in lettura ma non in scrittura. La modalità di sola lettura supporta l'accesso sicuro ai dati per una serie di casi d'uso dei clienti, tra cui audit, report e formazione.

Crittografia a riposo (applicazione cloud)

Quando i dati sono a riposo, il software Clarity LIMS utilizza il sistema di crittografia avanzato (AES, Advanced Encryption System)-256 per proteggere i dati. AES-256 è un noto sistema di crittografia facile da usare per gli sviluppatori, ma difficile da violare per gli hacker a causa della sua lunga chiave di 256 caratteri. AES-256 è utilizzato in modo affidabile nei settori finanziario, governativo e sanitario di tutto il mondo.

Crittografia in transito

Per proteggere i dati in transito, il software Clarity LIMS impiega il protocollo TLS (Transport Layer Security) 1.2 o versioni successive. TLS è una tecnologia standard e consolidata per sottoporre a crittografia le comunicazioni e lo scambio informativo tra un server web e un browser web. Proprio come la crittografia AES-256, il protocollo TLS viene utilizzato in modo affidabile in diversi settori, tra cui l'assistenza sanitaria.

Registrazione delle attività

In qualsiasi laboratorio, la tracciabilità dei campioni è importante, ma lo diventa ancora di più quando si lavora in ambienti basati sulla conformità. Il software Clarity LIMS rispetta la conformità producendo un audit trail di qualsiasi campione nel sistema.

Un audit trail è un resoconto dettagliato del campione e di ogni azione intrapresa sul campione dalla sua creazione in LIMS. I laboratori possono utilizzare l'audit trail prodotto dal software Clarity LIMS per generare un'adeguata reportistica sul sistema o per soddisfare i requisiti di audit. L'audit trail nel software Clarity LIMS descrive dettagliatamente tutti gli eventi nel corso della vita utile di un campione:

- Data e ora di acquisizione e caricamento del campione
- Utenti del laboratorio responsabili di eventuali azioni intraprese sul campione
- Reagenti utilizzati con il campione

Autenticazione

Il software Clarity LIMS utilizza un processo di autenticazione a singolo fattore. Gli utenti accedono tramite un portale web utilizzando le proprie credenziali. Le organizzazioni possono integrare la procedura delle password aziendali in modo che gli utenti di Clarity LIMS possano accedere utilizzando le password aziendali e protocollo LDAP (Lightweight Directory Access Protocol). L'integrazione con il protocollo LDAP è disponibile come parte del software Clarity LIMS Enterprise.

Gestione delle sessioni

Il software Clarity LIMS include una funzione di gestione delle sessioni per disconnettere automaticamente gli utenti dopo 30 minuti di inattività. La gestione delle sessioni può essere configurata dagli utenti con privilegi di amministratore.

Prevenzione delle vulnerabilità della rete e delle applicazioni

I controlli dei confini monitorano e regolano le comunicazioni, il confine esterno della rete e i principali confini interni. Questi controlli dei confini utilizzano set di regole, elenchi di controllo degli accessi e configurazioni per applicare il flusso di informazioni a specifici servizi del sistema informativo. Gli elenchi di controllo degli accessi, o politiche del flusso di traffico, sono stabilite su ciascuna interfaccia gestita per regolare il flusso di traffico. Ulteriori controlli includono:

- Scansione periodica della rete
- Politica contro l'uso delle e-mail per la consegna dei dati, che riduce i rischi associati agli allegati che potrebbero contenere malware
- Risposta prioritaria per problemi critici di sicurezza

Penetration test di terze parti

I penetration test di terze parti simulano un attacco alla distribuzione di un sistema e sono un ottimo metodo per testare attivamente le difese implementate. Illumina impiega una terza parte imparziale per condurre i penetration test delle istanze del cloud di Clarity LIMS. Dopo che il fornitore ha completato il test, Illumina riceve un report completo con i dettagli dei risultati. Illumina non divulga i risultati di questi penetration test.

Integrità dei dati*

Il backup del database del cliente avviene fino a 24 volte al giorno per ridurre il rischio di perdita di dati. Inoltre, il sistema contiene una registrazione che invia una notifica quando i dati vengono modificati. Se viene rilevata una modifica impropria, è possibile ripristinare una versione precedente sottoposta a backup.

Backup dei dati

Il cloud di Clarity LIMS viene sottoposto a una rigorosa procedura di backup per impedire la perdita di dati o disastri informatici. I dati vengono sottoposti a backup utilizzando un sistema automatizzato. Viene eseguito il backup del database, dei file di dati esterni associati e della configurazione di sistema appropriata. I backup sono crittografati in transito verso un'area di archiviazione S3 accessibile solo da personale autorizzato. Illumina conserva tre set di backup dal momento della loro creazione:

- Backup orari conservati per due giorni
- Backup giornalieri conservati per 32 giorni
- Backup mensili conservati per 400 giorni

Ripristino di emergenza

In caso di emergenza, verrà creato e configurato un nuovo sistema cloud e verrà recuperato un backup. Dopo l'implementazione del nuovo sistema, Illumina collaborerà con gli utenti del sistema per testare e assicurarsi che tutti i dati siano presenti.

Ogni anno pianifichiamo un test di ripristino di emergenza. Quando vengono rilasciate nuove versioni del software, è possibile che il piano di backup e ripristino di emergenza debba essere modificato. Qualsiasi modifica necessaria sarà apportata al sistema di backup e ripristino prima di attivare qualsiasi dato del cliente.

Conformità HIPAA

Il software Clarity LIMS è stato progettato e implementato per la conformità HIPAA. Il Congresso degli Stati Uniti ha emanato l'HIPAA nel 1996 e, successivamente, il Department of Health and Human Services degli Stati Uniti ha implementato diverse normative per l'applicazione della legge.[2] Tra le altre cose, l'HIPAA ha fissato gli standard nazionali per la sicurezza e la privacy delle PHI.

Le principali disposizioni previste dall'HIPAA includono la Regola di sicurezza e la Regola di notifica delle violazioni.

La Regola di sicurezza HIPAA stabilisce diversi requisiti per garantire la sicurezza e la privacy delle PHI. Il software Clarity LIMS include, a titolo esemplificativo ma non esaustivo, i requisiti di controllo della sicurezza (Tabella 1, Tabella 2).

GDPR

Il GDPR non si applica solo alle aziende con sede nell'Unione europea (UE). Anche le aziende con sede al di fuori dell'UE, ma che si rivolgono a individui nell'UE, possono essere soggette al GDPR.

In qualità di titolari del trattamento dei dati, i clienti sono in sostanza responsabili della valutazione dell'applicabilità del GDPR alle procedure di trattamento e dell'implementazione di prassi conformi al GDPR. Tuttavia, dato che il GDPR è rilevante per molti dei nostri clienti, Clarity LIMS si attiene ai principi del GDPR applicabili ai responsabili del trattamento dei dati.

Responsabilità condivise

Illumina è responsabile della protezione dell'infrastruttura su cui sono in esecuzione tutti i servizi offerti in AWS Cloud. Questa infrastruttura è composta da hardware, software, rete e strutture su cui sono in esecuzione i servizi AWS Cloud. Nel rispetto di tale responsabilità Illumina è tenuta a eseguire aggiornamenti ricorrenti delle patch di sicurezza o altri aggiornamenti per proteggere l'ambiente dalle minacce emergenti e favorire miglioramenti iterativi. Illumina fornisce questi aggiornamenti durante le finestre settimanali definite nei Termini e condizioni previsti nel software Clarity LIMS. I clienti tenuti a rispettare l'HIPAA hanno la responsabilità di garantire che dispongano di un programma di conformità HIPAA.

Controlli di sicurezza

L'utilizzo del software Clarity LIMS pone diverse responsabilità nelle mani del cliente. La valutazione del rischio deve tenere conto dell'uso delle soluzioni software come servizio (SaaS, Software as a Service) e i risultati di queste valutazioni devono essere riportati in una revisione dei controlli di privacy e sicurezza di ciascun cliente. I clienti devono rivedere le proprie politiche per riflettere l'uso del software Clarity LIMS.

* Le mitigazioni tramite integrità dei dati, backup dei dati e ripristino di emergenza vengono eseguite solo per il software cloud di Clarity LIMS.

Gli istituti devono stabilire processi e procedure per l'approvazione degli accessi e implementare revisioni regolari degli accessi accordati a tutti gli utenti. Inoltre, le workstation utilizzate per accedere al software Clarity LIMS devono disporre di protezioni adeguate, come software antivirus, firewall basati su host e registrazione centralizzata. I piani di continuità operativa aziendale e per il ripristino di emergenza devono essere aggiornati con lo scopo di tenere conto dell'uso del software Clarity LIMS.

Tabella 2. Controlli di sicurezza nel software Clarity LIMS

Controlli amministrativi
Politiche e procedure per prevenire, rilevare, contenere e correggere le violazioni della sicurezza
Funzionario della sicurezza responsabile dello sviluppo e dell'implementazione dei controlli all'interno dell'organizzazione
Procedure per garantire che l'accesso ai dati da parte dei dipendenti sia appropriato e approvato
Impostazione delle autorizzazioni di accesso di sola lettura
Procedure per autorizzare l'accesso ai dati dei clienti
Membri del personale formati sull'HIPAA
Procedure di segnalazione degli incidenti
Valutazione di routine per determinare l'impatto sulla sicurezza delle modifiche ad altre procedure o all'ambiente
Controlli fisici
Implementazione del controllo degli accessi alla struttura
Software Clarity LIMS ospitato in data center sicuri
Politiche sulla sicurezza delle workstation
Controlli tecnici
ID utente univoco per ciascun utente
Autenticazione utente mediante il software Clarity LIMS o LDAP di un cliente
Crittografia dei dati in transito e a riposo

Risposta agli incidenti e notifica delle violazioni

Ai sensi dell'HIPAA, i partner commerciali sono tenuti a rispettare una serie di regole e normative relative alle violazioni potenziali e reali. Se si è verificato un tentativo di violazione, Illumina completerà una valutazione del rischio per determinare se il tentativo costituisce una violazione reale. In tal caso, Illumina informerà il cliente non appena ragionevolmente possibile, a condizione che i tentativi non andati a buon fine, come ping e altri attacchi di trasmissione sul nostro firewall, scansioni delle porte, tentativi di accesso non riusciti, attacchi denial of service e qualsiasi combinazione degli eventi descritti sopra, non costituiscano un tentativo di violazione.

Conformità del laboratorio

Il software Clarity LIMS include numerose funzionalità per garantire la conformità a normative, standard e certificazioni applicabili ai laboratori che eseguono i test su campioni umani, come CLIA, CAP e ISO 15189. Eccone alcune:

- Monitoraggio dei campioni e cronologia completa dei campioni per scopi di audit
- Strumenti che contribuiscono al rispetto delle procedure operative standard
- Monitoraggio di reagenti e lotti
- Interfacce basate sui ruoli che consentono l'accesso solo alle funzioni autorizzate
- Funzionalità di sicurezza, come descritto in questa nota tecnica

Maggiori informazioni

Software Clarity LIMS

Bibliografia

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

illumina®

Numero verde 1.800.809.4566 (U.S.A.) | Tel. +1.858.202.4566
techsupport@illumina.com | www.illumina.com

M-GL-00704 ITA v3.0