NOTE TECHNIQUE

Sécurité, confidentialité et conformité de Clarity LIMS[MC]

Les fonctionnalités et l'approche qui aident à protéger vos données

illumina[MD]

Promouvoir des pratiques rigoureuses en matière de sécurité et de confidentialité

Préserver la confidentialité des renseignements protégés sur la santé (RPS), notamment des données génomiques, est essentiel aux opérations commerciales mondiales d'Illumina. Notre approche de la protection et de la confidentialité des données, telle qu'elle est décrite dans notre Politique de confidentialité d'entreprise, s'aligne sur les normes clés définies par les réglementations nationales et mondiales en matière de confidentialité des données, notamment la loi américaine sur l'assurance maladie (HIPAA, Health Insurance Portability and Accountability Act), le Règlement général sur la protection des données (RGPD) et la loi californienne sur la protection de la vie privée des consommateurs (CCPA, California Consumer Privacy Act). Nous nous engageons à respecter les principes directeurs suivants :

- **Transparence** : nous communiquons clairement nos pratiques en matière de confidentialité et la façon dont nous utilisons les données personnelles.
- **Gérance responsable** : nous assurons la protection des données personnelles afin de préserver leur confidentialité et leur sécurité.
- **Usage éthique** : nous recueillons et utilisons des données personnelles uniquement de manière légale et transparente à des fins qui renforcent notre mission qui consiste à améliorer la santé humaine en exploitant le pouvoir du génome.
- **Responsabilité** : nous nous engageons à respecter toutes les exigences légales et à promouvoir nos pratiques internes afin d'atteindre les normes les plus élevées en matière de confidentialité des données personnelles.

Cadres de sécurité

Des pratiques institutionnelles rigoureuses en matière de confidentialité reposent sur un programme de sécurité des renseignements efficace. Bien qu'il y ait plusieurs cadres de sécurité en place à l'échelle mondiale, nos pratiques et cette note technique se concentrent sur les cadres les plus courants, notamment :

- l'HIPAA;
- l'Organisation internationale de normalisation (ISO, International Organization for Standardization) 27001 (sécurité) et 27701 (confidentialité).

Infrastructure

Illumina applique ses propres contrôles et procédures de sécurité pour la sécurité de Clarity LIMS (système de gestion des informations de laboratoire) ainsi qu'une approche complète et éprouvée héritée d'Amazon Web Services (AWS) (figure 1)[1].

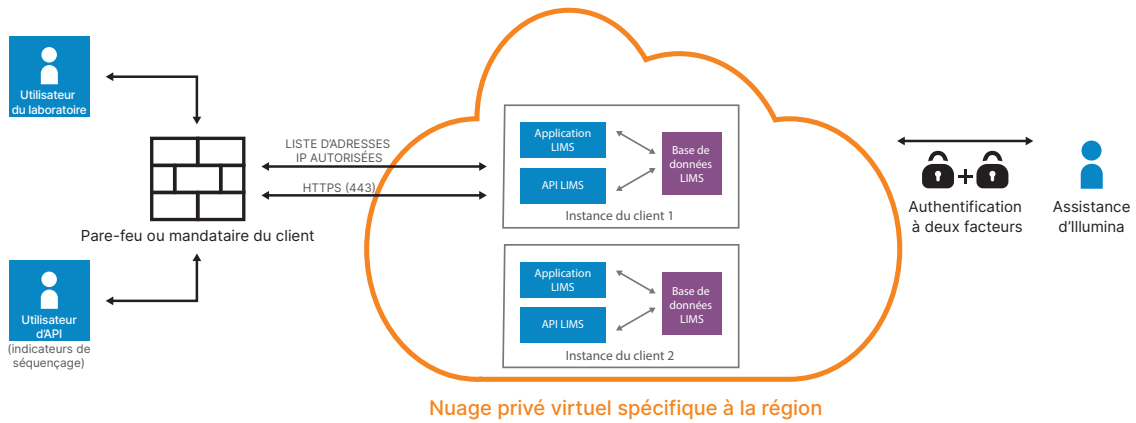

Figure 1 : L'infrastructure de sécurité du logiciel Clarity LIMS.

Aperçu des contrôles de sécurité

Un aperçu général des contrôles de sécurité intégrés dans le logiciel Clarity LIMS est fourni dans le tableau 1. Des renseignements détaillés sont fournis dans le reste de cette note technique.

Tableau 1 : Liste de vérification relative à la sécurité et à la confidentialité de Clarity LIMS

Vérifications internes et procédurales			
Vérification des antécédents des employés	✓	Surveillance	✓
Politiques de sécurité	✓	Réponse aux incidents	✓
Contrôle des accès	✓	Application anti-programme malveillant	✓
Accès en lecture seule attribuable au rôle	✓	Plans de reprise après sinistre	✓
Sauvegardes	✓		
Application infonuagique			
Contrôle des accès	✓	Application anti-programme malveillant	✓
Chiffrement au repos	✓	Reprise après sinistre	✓
Chiffrement en transit	✓	Sauvegarde des données	✓
Enregistrement de l'activité	✓	Intégrité des données	✓
Test d'intrusion tiers	✓	Examen/test du code	✓
Contrôle d'accès basé sur le rôle	✓	Réseau	✓
Contrôles du mot de passe	✓	Segmentation du réseau	✓
Gestion des sessions	✓		
Conformité et attestation – Version 5.4 et versions ultérieures			
ISO/CEI 27001:2013 (pour les instances en nuage)	✓	HIPAA (validée par un tiers)	✓
ISO/CEI 27701:2019 (pour les instances en nuage, v6.1 et ultérieures)	✓		

Pratiques de sécurité relatives aux employés

Nos pratiques de sécurité commencent avant l'arrivée des nouveaux employés. Nous vérifions les antécédents de tous les candidats lorsque cela est permis par la loi. Les politiques documentées guident le personnel dans la prévention, la détection et le contrôle de toute atteinte à la sécurité.

Un programme de sensibilisation et de formation à la sécurité communique les politiques de sécurité aux employés qui développent ou utilisent le logiciel Clarity LIMS. Un système de formation automatisé garantit que tous les employés requis suivent cette formation.

Tous les employés qui utilisent le logiciel Clarity LIMS doivent suivre une formation annuelle sur la façon de gérer les données des clients. L'accès aux systèmes des clients est accordé aux employés nécessaires. Le téléchargement des données est limité et toutes les activités sont enregistrées et documentées dans un système automatisé. Lorsque les employés qui ont utilisé le logiciel Clarity LIMS quittent l'entreprise, leur accès à tous les systèmes des clients et aux systèmes internes d'Illumina est révoqué. Tous les équipements et les badges fournis à l'employé sont retournés.

Mesures associées à l'établissement

ISO/CEI 27001:2013 et ISO/CEI 27701:2019 pour Clarity LIMS sur le nuage

La norme ISO 27001:2013 est une norme relative au système de gestion de la sécurité des renseignements (ISMS, Information Security Management System) qui vise à placer toute la gestion de la sécurité de l'information sous la gouvernance de la direction, en veillant à ce que les processus et les politiques soient déployés et appliqués de manière cohérente et fiable. La norme dicte la façon dont les données sont stockées et gérées et dont les actifs informationnels sont éliminés. La norme ISO/CEI 27701:2019 est une norme relative au système de gestion de la protection de la vie privée (PIMS, Privacy Information Management System) qui certifie que des exigences strictes en matière de confidentialité des données sont mises en œuvre pour le stockage et la conservation des données de manière confidentielle et conforme. Les politiques en vigueur pour les normes ISO/CEI 27001:2013 et ISO/CEI 27701:2019 établissent également des normes pour le contrôle d'accès, la gestion des mots de passe et la sécurité du réseau.

Certification ISO d'Illumina

HIPAA

Les établissements dans lesquels les RPS sont traités sont conformes à l'HIPAA et aux meilleures pratiques du secteur. Exemples des meilleures pratiques que nous suivons :

- Les bâtiments sont surveillés 24 heures sur 24 et accessibles par carte-clé.
- Les bureaux disposent d'un système de sécurité surveillé.
- Les ordinateurs utilisés pour accéder aux RPS ou les stocker sont protégés par un mot de passe et le chiffrement complet du disque est activé.
- Tout accès depuis l'extérieur du bureau se fait par l'entremise d'un réseau privé virtuel (VPN, Virtual Private Network) sécurisé.

Développement de Clarity LIMS

Le logiciel Clarity LIMS est développé et testé pour offrir une expérience fiable, utilisable et prévisible aux utilisateurs. Le processus de développement de logiciels détermine la hiérarchisation des fonctionnalités et des corrections de bogues en fonction des besoins de l'entreprise et des commentaires du client. Nous utilisons une méthodologie Agile pour développer le logiciel Clarity LIMS. Le manifeste Agile est mis en œuvre par Scrum, une méthode très répandue et acceptée pour exécuter le processus de développement.

Les principales fonctionnalités d'Agile comprennent : des cycles de développement courts appelés sprints, la capacité à modifier les besoins commerciaux et techniques et à s'y adapter, ainsi qu'un examen et des améliorations constants du processus. À l'achèvement, tous les changements de code sont examinés par au moins deux autres développeurs, sauf dans le cas de petits changements de formulation. Le processus d'examen aide les développeurs à identifier les problèmes dans la base de code ou l'utilisation de modèles de code non conformes aux normes. Les codes non conformes aux normes seront révisés et examinés jusqu'à ce qu'ils soient conformes. La méthodologie Agile offre plusieurs points de contrôle conçus pour fournir un système qui répond aux attentes des clients ou qui les dépasse. Cette mesure et d'autres mesures d'assurance qualité, telles que la vérification automatisée du code, garantissent que les systèmes livrés correspondent aux fins prévues et que les processus utilisés sont corrects et appropriés.

Mise en œuvre et mises à jour de Clarity LIMS sur le nuage

De temps à autre, Illumina publiera des correctifs de sécurité et de système d'exploitation (SE), des corrections de bogues et d'autres versions. Lorsque les versions de correctifs de sécurité et de Clarity LIMS seront publiées, Illumina mettra à jour les instances Clarity LIMS applicables pendant les intervalles programmés. Dans le cadre de nos activités de correction, les éléments suivants peuvent être mis à niveau :

- les correctifs de SE sous-jacents;
- les correctifs logiciels ou Clarity LIMS sous-jacents inclus;
- les outils d'Illumina, notamment les antivirus, la journalisation, la détection des intrusions, les sauvegardes, etc.;
- les composants supplémentaires du système qui n'affectent pas la fonctionnalité standard de Clarity LIMS pour la version déployée.

Pour les mises à jour mineures et majeures, le personnel d'Illumina coordonne le calendrier des mises à niveau avec les clients et fournit des notifications de fin de vie, d'hébergement et d'assistance pour les versions plus anciennes. Illumina applique généralement les versions de correctifs à toutes les versions hébergées applicables pendant les intervalles programmés, à moins que les exigences de sécurité ou autres ne demandent une réponse plus rapide. À la fin de l'hébergement, Illumina peut mettre à niveau les versions antérieures qui n'ont pas encore été mises à niveau vers la dernière version de Clarity LIMS.

Pratiques de sécurité au sein du logiciel Clarity LIMS

Le logiciel Clarity LIMS comprend plusieurs fonctionnalités et mesures pour promouvoir la sécurité et la confidentialité des RPS.

Contrôle des accès

Les travaux en laboratoire nécessitent du personnel doté d'un ensemble diversifié de compétences et qui effectue de nombreuses tâches. Pour éviter les erreurs, la perte de données ou le sabotage, l'accès au système est limité en fonction des rôles. Le logiciel Clarity LIMS comprend un contrôle d'accès configurable, avec la possibilité de configurer un accès en lecture seule à l'aide des paramètres d'autorisation basés sur les rôles (disponible à partir de Clarity LIMS v6.1).

Les utilisateurs avec des rôles d'administrateur peuvent configurer l'accès de sorte que les utilisateurs désignés aient un accès en lecture, mais pas en écriture. Le mode lecture seule prend en charge l'accès sécurisé aux données pour un éventail de cas d'utilisation client, notamment la vérification, l'établissement de rapports et la formation.

Chiffrement au repos (application infonuagique)

Lorsque les données sont au repos, le logiciel Clarity LIMS utilise la norme de chiffrement avancé (AES)-256 pour assurer la protection des données. AES-256 est un système de chiffrement bien connu, facile à utiliser pour les développeurs, mais difficile à craquer pour les pirates informatiques en raison de sa longue clé de 256 caractères. AES-256 est utilisé en toute confiance dans les secteurs de la finance, du gouvernement et des soins de santé à travers le monde.

Chiffrement en transit

Pour protéger les données en transit, le logiciel Clarity LIMS utilise le protocole de sécurité de la couche transport (TLS, Transport Layer Security) 1.2 ou une version plus récente. Le protocole TLS est une technologie standard et éprouvée pour le chiffrement de la liaison entre un serveur Web et un navigateur Web. Tout comme la norme de chiffrement avancé (AES)-256, le protocole TLS est utilisé en toute confiance dans de nombreux secteurs, notamment celui des soins de santé.

Enregistrement de l'activité

Pour tous les laboratoires, la traçabilité des échantillons est importante, mais elle l'est encore plus dans des environnements axés sur la conformité. Le logiciel Clarity LIMS garantit la conformité en générant une piste de vérification de l'ensemble des échantillons du système.

Une piste de vérification est un compte rendu détaillé de l'échantillon et de toutes les actions réalisées sur l'échantillon depuis sa création dans le LIMS. Les laboratoires peuvent utiliser la piste de vérification générée dans le logiciel Clarity LIMS pour faciliter l'établissement de rapports du système ou pour satisfaire aux exigences en matière de vérification. La piste de vérification du logiciel Clarity LIMS détaille tous les événements survenus au cours de la durée de vie d'un échantillon :

- la date et l'heure d'acquisition et de téléversement de l'échantillon;
- les utilisateurs du laboratoire responsables des actions réalisées sur l'échantillon;
- les réactifs utilisés avec l'échantillon.

Authentification

Le logiciel Clarity LIMS utilise un processus d'authentification à facteur unique. Les utilisateurs se connectent par l'entremise d'un portail Web à l'aide de leurs identifiants. Les organisations peuvent intégrer leur processus de mots de passe d'entreprise afin que les utilisateurs de Clarity LIMS puissent se connecter à l'aide de leurs mots de passe d'entreprise et du protocole allégé d'accès annuaire (LDAP, Lightweight Directory Access Protocol). L'intégration avec le protocole LDAP est disponible dans le cadre du logiciel Clarity LIMS Enterprise.

Gestion des sessions

Le logiciel Clarity LIMS comprend une fonction de gestion des sessions qui permet de déconnecter automatiquement les utilisateurs après 30 minutes d'inactivité. La gestion des sessions peut être configurée par les utilisateurs disposant de droits d'administrateur.

Prévention des vulnérabilités du réseau et des applications

Les contrôles des limites permettent de surveiller et de réglementer les communications, les limites externes du réseau et les principales limites internes. Ces contrôles des limites utilisent des ensembles de règles, des listes de contrôle d'accès et des configurations pour appliquer le flux de renseignements à des services de systèmes informatiques spécifiques. Des listes de contrôle d'accès, ou des politiques de flux de trafic, sont établies sur chaque interface gérée pour réguler le trafic. Les contrôles supplémentaires comprennent :

- l'analyse périodique du réseau;
- la politique contre l'utilisation des courriels pour la transmission des données, réduisant ainsi les risques associés aux pièces jointes qui pourraient contenir des logiciels malveillants;
- une réponse hiérarchisée aux problèmes de sécurité critiques.

Tests d'intrusion tiers

Les tests d'intrusion tiers simulent une attaque sur le déploiement d'un système et constituent un bon moyen de tester activement les défenses. Illumina fait appel à un tiers impartial pour effectuer des tests d'intrusion pour les instances en nuage de Clarity LIMS. Une fois que le fournisseur a terminé le test, Illumina reçoit un rapport complet détaillant les résultats. Illumina ne publie pas les résultats de ces tests d'intrusion.

Intégrité des données*

La sauvegarde de la base de données client a lieu jusqu'à 24 fois par jour pour réduire le risque de perte de données. En outre, le système contient une journalisation qui fournit des notifications lorsque les données sont modifiées. Si une modification incorrecte est détectée, il est possible de revenir à une version de sauvegarde précédente.

Sauvegardes des données

Clarity LIMS en nuage est soumis à un processus de sauvegarde rigoureux pour le protéger contre la perte de données ou les sinistres. Les données sont sauvegardées à l'aide d'un système automatisé. La base de données, les fichiers de données externes associés et la configuration système appropriée sont sauvegardés. Les sauvegardes sont chiffrées en transit vers une zone de stockage S3 accessible uniquement par le personnel autorisé. Illumina conserve trois ensembles de sauvegardes à partir de leur création :

- les sauvegardes horaires conservées pendant deux jours;
- les sauvegardes quotidiennes conservées pendant 32 jours;
- les sauvegardes mensuelles conservées pendant 400 jours.

Reprise après sinistre

En cas de sinistre, un nouveau système infonuagique sera créé et configuré et une sauvegarde sera restaurée. Une fois le nouveau système mis en œuvre, Illumina travaillera avec les utilisateurs du système pour le tester et s'assurer que toutes les données sont présentes.

Nous planifions un test de reprise après sinistre chaque année. Au fur et à mesure que de nouvelles versions du logiciel sont publiées, il est possible que le plan de sauvegarde et de reprise après sinistre doive être modifié. Toutes les modifications nécessaires seront apportées au système de sauvegarde et de reprise avant la mise en service des données client.

Conformité à l'HIPAA

Le logiciel Clarity LIMS a été conçu et mis en œuvre pour être conforme à l'HIPAA. Le Congrès des États-Unis a promulgué l'HIPAA en 1996, puis le département de la Santé et des Services sociaux des États-Unis a mis en œuvre plusieurs réglementations pour appliquer la loi[2]. L'HIPAA a, entre autres, établi des normes nationales pour la sécurité et la confidentialité des RPS. Les principales dispositions de l'HIPAA comprennent la règle de sécurité informatique et la règle de notification des violations.

La règle de sécurité informatique de l'HIPAA impose plusieurs exigences pour assurer la sécurité et la confidentialité des RPS. Le logiciel Clarity LIMS comprend, sans s'y limiter, les exigences en matière de contrôle de sécurité (tableau 1, tableau 2).

RGPD

Le RGPD ne s'applique pas uniquement aux entreprises implantées dans l'UE. Les entreprises implantées en dehors de l'UE, mais qui ciblent des individus résidant dans l'UE, peuvent également être soumises au RGPD.

En tant que responsables du traitement des données, les clients sont, en définitive, responsables de l'évaluation de l'applicabilité du RGPD à leurs opérations de traitement et de s'assurer qu'ils ont mis en place une pratique conforme au RGPD. Cependant, étant donné que le RGPD est pertinent pour bon nombre de nos clients, Clarity LIMS respecte les principes du RGPD applicables aux préposés au traitement des données.

Responsabilités partagées

Illumina est responsable de la protection de l'infrastructure qui exécute l'ensemble des services offerts dans le nuage AWS. Cette infrastructure est composée du matériel, des logiciels, de la mise en réseau et des établissements qui exécutent les services infonuagiques AWS. Une partie de cette responsabilité exige qu'Illumina effectue des mises à jour de correctifs de sécurité récurrentes ou d'autres mises à jour pour protéger l'environnement des menaces émergentes et mettre en place des améliorations progressives. Illumina fournit ces mises à jour pendant les intervalles hebdomadaires définis dans les conditions générales du logiciel Clarity LIMS. Les clients tenus de se conformer à l'HIPAA doivent s'assurer d'avoir mis en place un programme de conformité à l'HIPAA.

Contrôles de sécurité

L'utilisation du logiciel Clarity LIMS implique pour le client d'assumer plusieurs responsabilités. L'évaluation des risques doit tenir compte de l'utilisation de solutions de logiciel-service (SaaS, Software as a Service) et les résultats de cette évaluation doivent être reflétés dans un examen des contrôles de confidentialité et de sécurité de chaque client. Les clients doivent examiner leurs politiques pour refléter l'utilisation du logiciel Clarity LIMS. Les institutions doivent établir des processus et des procédures pour l'approbation de l'accès et mettre en œuvre des examens réguliers de l'accès qui a été accordé à tous les utilisateurs.

* Les méthodes d'atténuation relatives à l'intégrité des données, à la sauvegarde des données et à la reprise après sinistre concernent uniquement le logiciel Clarity LIMS en nuage.

De plus, les postes de travail utilisés pour accéder au logiciel Clarity LIMS doivent disposer de protections appropriées, telles qu'un logiciel antivirus, des ordinateurs coupe-feu et une journalisation centralisée. Les plans de continuité des activités et de reprise après sinistre doivent être mis à jour pour tenir compte de l'utilisation du logiciel Clarity LIMS.

Tableau 2 : Contrôles de sécurité au sein du logiciel Clarity LIMS

Contrôles administratifs
Politiques et procédures pour prévenir, détecter, contenir et corriger les atteintes à la sécurité
Responsable de la sécurité chargé du développement et de la mise en œuvre des contrôles au sein de l'organisation
Procédures pour garantir que l'accès aux données par les membres du personnel est approprié et approuvé
Paramètre d'autorisation d'accès en lecture seule
Processus pour autoriser l'accès aux données des clients
Membres du personnel formés à l'HIPAA
Processus de signalement des incidents
Évaluation de routine pour déterminer comment les changements apportés à d'autres procédures ou à l'environnement peuvent potentiellement avoir un impact sur la sécurité
Contrôles physiques
Mise en œuvre des contrôles d'accès dans les établissements
Logiciel Clarity LIMS hébergé dans des centres de données sécurisés
Politiques relatives à la sécurité des postes de travail
Contrôles techniques
ID utilisateur unique pour chaque utilisateur
Authentification de l'utilisateur par le logiciel Clarity LIMS ou le protocole LDAP d'un client
Chiffrement des données en transit et au repos

Réponse aux incidents et notification des violations

En vertu de l'HIPAA, les partenaires commerciaux sont tenus de se conformer à un ensemble de règles et de réglementations concernant les violations potentielles et réelles. Lors d'une tentative de violation, Illumina effectue une évaluation des risques pour déterminer si la tentative constitue une violation réelle. Si tel est le cas, Illumina informe le client le plus rapidement possible, à condition que les tentatives infructueuses, telles que les pings et autres attaques informatiques sur notre pare-feu, le scannage de ports, les tentatives de connexion infructueuses, les attaques par déni de service et toute combinaison des éléments ci-dessus, ne constituent pas une tentative de violation.

Conformité du laboratoire

Le logiciel Clarity LIMS comprend de nombreuses fonctionnalités pour assurer la conformité aux réglementations, aux normes et aux conditions d'agrément applicables aux laboratoires qui effectuent des tests sur des échantillons humains, comme CLIA, CAP et ISO 15189. Ces fonctionnalités comprennent :

- le suivi des échantillons et l'historique complet des échantillons à des fins de vérification;
- des outils qui aident à se conformer aux procédures normales d'exploitation;
- le suivi des réactifs et des lots;
- des interfaces basées sur les rôles qui permettent d'accéder uniquement aux fonctions autorisées;
- des fonctions de sécurité, comme décrit dans cette note technique.

En savoir plus

Logiciel Clarity LIMS

Références

1. Amazon Web Services. AWS Cloud Security. aws.amazon.com/security/. Consulté le 28 janvier 2023.
2. US Department of Health & Human Services. Summary of the HIPAA Privacy Rule. hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Mis à jour le 26 juillet 2013. Consulté le 28 janvier 2023.
3. Centers for Medicare & Medicaid Services. cms.gov/. Consulté le 28 janvier 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. Mis à jour le 1er décembre 2021. Consulté le 28 janvier 2023.
5. College of American Pathologists. Accreditation. cap.org/laboratory-improvement/accreditation. Consulté le 28 janvier 2023.

illumina[MD]

Numéro sans frais aux États-Unis : + (1) 800 809-4566 | Téléphone : + (1) 858 202-4566
techsupport@illumina.com | www.illumina.com

M-GL-00704 FRA v3.0