dicma
Gestion Documentaire de Dictée

Corti

Sécurité et Gouvernance

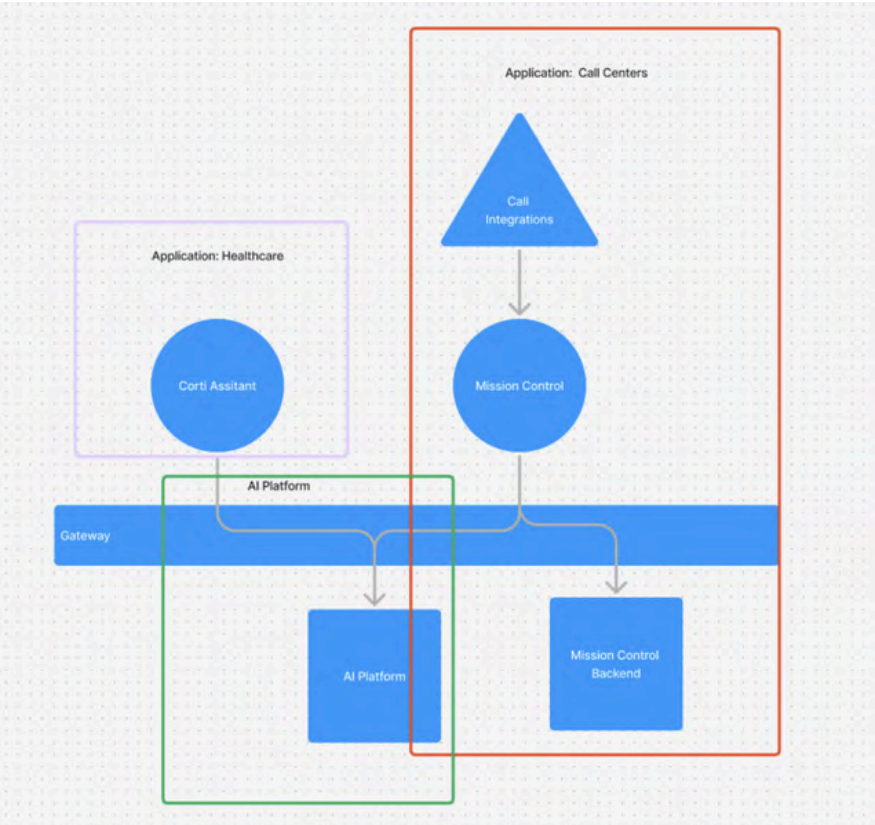
Contactez-nous: dicma@dicma.fr www.dicma.fr

Table des matières

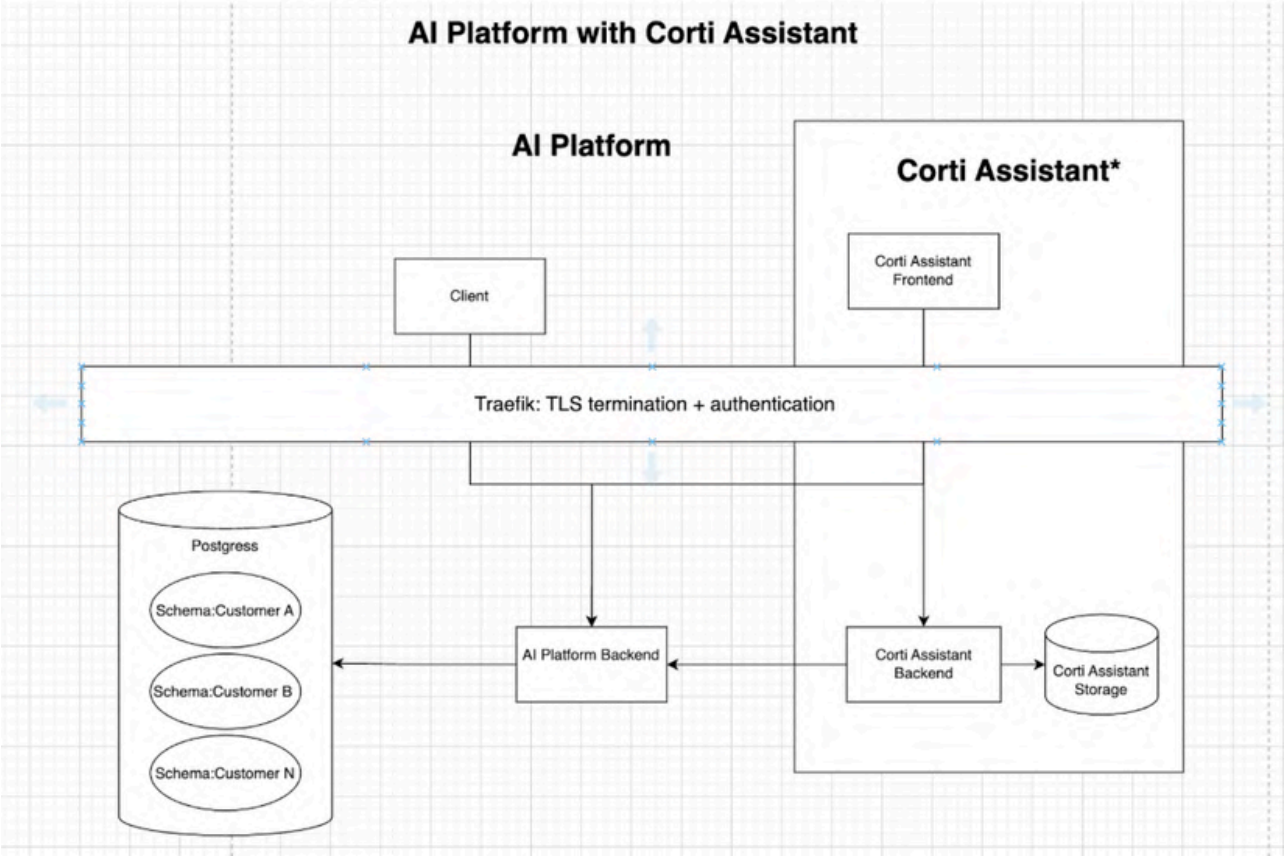
Architecture du Système

L'offre de solutions Corti fournit aux professionnels de santé des capacités d'IA qui optimisent leur travail quotidien, notamment grâce à une assistance disponible à tout moment. L'offre est divisée en trois lignes de produits :

- Plate-forme d'IA : un produit API qui exploite les capacités d'IA par le biais d'une interface système facile à utiliser.
- Applications Santé construite à partir de la Plateforme IA. Elle combine les données de sortie encapsulées en flux de travail dans diverses interfaces utilisateur.
  La solution principale est une Application React appelée Corti Assistant.
- Applications Centres d'Appels : ce produit aligne les lignes d'urgence dans les hôpitaux, les services d'incendie et les services de police. Il offre diverses intégrations pour les données d'appel. Il est partiellement construit sur la Plateforme IA et est destiné à être entièrement migré. Il existe un ensemble de modèles d'IA internes à l'application.



Plateforme IA

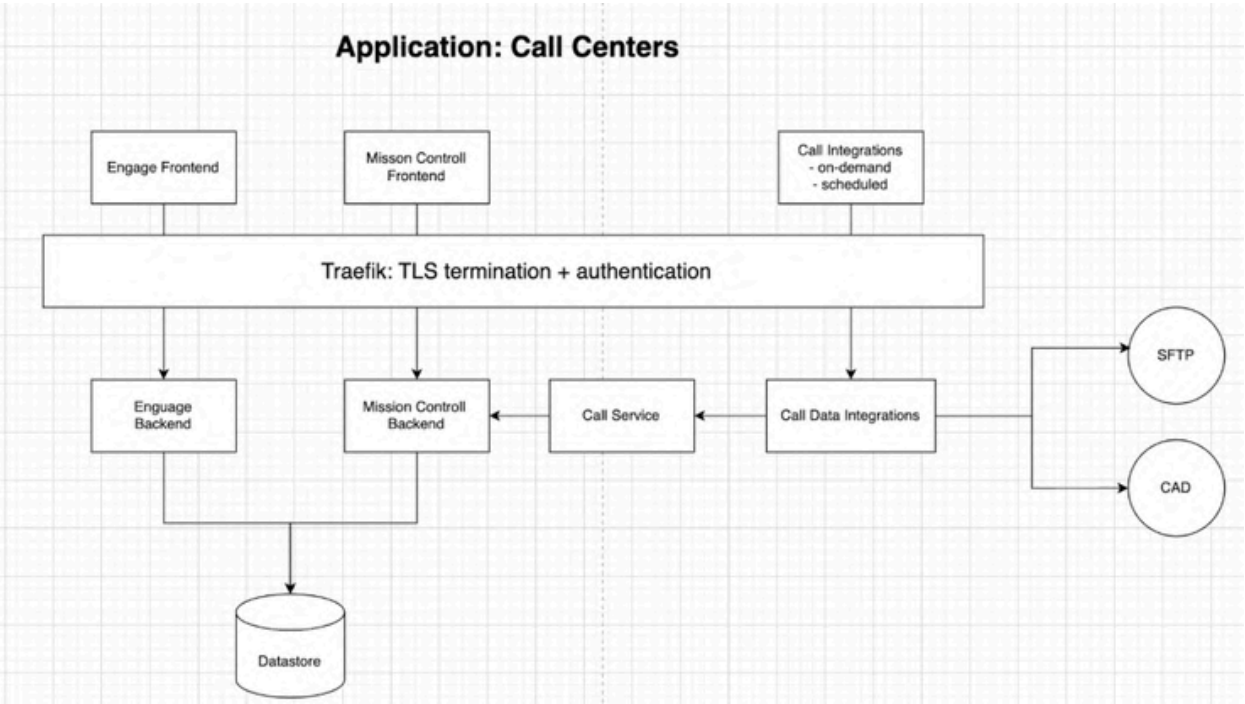


Dans la figure ci-dessus, la zone désignée comme "Corti Assistant" est optionnelle. Elle n'est pas obligatoire, mais dépend de l'accord sur le produit. Les clients ont la possibilité d'intégrer directement la plateforme d'IA ou de recevoir un produit prêt à l'emploi qui exploite toutes les capacités de cette dernière.
Corti Assistant a été optimisé pour offrir une expérience utilisateur de haute qualité.

Application : santé

Décrit dans la section de la plateforme IA.

Application : centres d'appels



Déploiement

Nous livrons la solution Corti en tant que service cloud sécurisé à nos clients. Cette approche nous permet de configurer chaque instance de service déployée pour répondre aux besoins de nos clients avec flexibilité, évolutivité et résilience.

Service Corti

Corti livre sa solution en tant que service entièrement géré hébergé dans l'environnement cloud virtuel sécurisé d'Azure.

Chacune des solutions de Corti est déployée dans un centre de données Azure géographiquement optimisé pour répondre aux exigences réglementaires et juridictionnelles. Nous configurons les instances Azure pour fournir aux clients une infrastructure entièrement gérée et sécurisée.

Cette approche offre une solution évolutive utilisant une infrastructure entièrement maintenue et sécurisée. Nous employons deux stratégies de déploiement client : une installation multi-tenant ou spécifique au client. La stratégie dépend de l'offre de produit choisie par le client.

Aperçu de la Sécurité et de la Gouvernance de Corti

Les clients utilisant notre Plateforme IA ou nos Applications Santé sont hébergés dans un environnement multi-tenants, tandis que les clients utilisant nos Applications Centres d'Appels bénéficient d'un environnement autonome.

Les deux stratégies sont conçues de manière à ce que toutes les fonctions de gestion des données, y compris le contrôle de la sécurité de l'information, les opérations de sauvegarde et de récupération, la journalisation et l'audit, soient invisibles pour le client.
Par conséquent, ces services éliminent le besoin de spécialistes internes pour exploiter et maintenir la solution. Nous offrons un tableau de bord et une API orientés clients pour les informer de l'état du système.

L'accès client est fourni via une application Web, un installateur Microsoft Windows ou une API, selon la préférence du client. La différence dans la gestion des données entre multi-tenant et autonome est l'isolation des données. Basée sur le schéma pour multi-tenant et basée sur le serveur pour plus d'autonomie.

Détails du Service
Gestion des Accès : les clients accèdent à Corti via nos passerelles API. Pour la Plateforme IA et Applications : santé, nous employons une passerelle API régionale pour chacun de nos environnements multi-tenants régionaux.

Pour Applications : centres d'Appels, nous employons une passerelle API pour chaque environnement dédié.
Connectivité : Corti utilise le proxy inverse Traefik et la solution de répartition de charge pour mettre en œuvre des connexions sécurisées entre les clients et le service hébergé sur Azure en utilisant un protocole de sécurité de la couche de transport (TLS). Les protocoles de communication employés incluent :

- Hypertext Transfer Protocol Secure (HTTPS) pour les applications de service externes, y compris les interfaces de programmation d'applications (API), les applications clientes sur les dispositifs des utilisateurs finaux (EUD) et les métadonnées des systèmes de diagnostic assisté par ordinateur (CAD)

- SSH File Transfer Protocol (SFTP) pour les données d'appel et les métadonnées associées. SSH est le protocole Secure Shell, un protocole réseau cryptographique pour exploiter des services en toute sécurité sur un réseau non sécurisé tel qu'Internet.

Gestion des Clés : Corti utilise Terraform, la solution d'infrastructure entant que code pour créer et gérer en toute sécurité les clés cryptographiques de chaque client. Nous contrôlons strictement l'accès aux clés en utilisant la technologie de gestion des accès basée sur les rôles d'Azure et avons une seule paire de clés SSH par tenant. De plus, l'utilisation des clés est auditée et journalisée dans le cadre de la gestion de la solution gérée.

Gestion du Contenu : nous protégeons les instances de service client contre l'entrée de contenu malveillant, y compris les logiciels malveillants, en imposant des contrôles sur les types de contenu autorisés et en limitant les connexions aux plages d'IP approuvées en utilisant des techniques de liste blanche d'IP.

Pour les Applications : santé, nous autorisons le trafic entrant d'un ensemble de pays autorisés, et pour les Applications : centres d'Appels, nous autorisons un ensemble convenu de plages CIDR sur une base client par client.

Base de Données SQL

Présent dans : environnements multi-tenants et autonomes

Corti fournit à nos clients une base de données SQL Azure en tant que service cloud géré pour le stockage de données structurées.

Cette installation offre les avantages de la fonctionnalité SQL dans un service entièrement géré.

La base de données SQL Azure offre :

- Des contrôles de sécurité multicouches avancés, y compris la sécuritéeréseau, le chiffrement des données, la gestion des accès et des clés, laeprotection contre les menaces en temps réel, l'alerte proactive desevulnérabilités et la vérification

- Un pare-feu de base de données SQL Azure qui gère le contrôle d'accèsedes données stockées

- Un provisionnement automatique qui optimise la configuration tout en garantissant la conformité aux normes réglementaires, y compris HIPAA et GDPR
- Des mises à jour automatiques pour réduire la fenêtre de risque pour les vulnérabilités connues sans imposer de surcharge administrative

- Sauvegarde automatique des informations importantes dans le cadre des pratiques de récupération d'incidents et de continuité des activités

- Une évolutivité flexible pour répondre aux besoins de croissance
- Une haute disponibilité avec des options de niveau de service allant jusqu'à une garantie de 99,995 %

Azure Blob Data Lake

Présent dans : environnements multi-tenant et autonomes

Les clients de la solution Corti peuvent choisir d'utiliser le stockage Azure Blob en tant que service cloud géré pour le stockage en vrac de données non structurées. Cette installation offre l'avantage de créer des lacs de données dans un service entièrement géré encapsulé dans l'instance Corti du client.

Le Azure Blob Data Lake offre :

- La sécurité des données avec l'authentification basée sur les rôles d'Azure Active Directory, le chiffrement des données et la protection avancée contre les menaces
- Des capacités de stockage massif des données avec une évolutivité rentable
- Un accès multi-protocole et une prise en charge de l'espace de noms de fichiers
- Une gestion des données de bout en bout utilisant des contrôles d'accès basés sur des politiques
- Un stockage à faible latence pour répondre aux exigences de haute performance
- Une prise en charge la sauvegarde des informations importantes dans le cadre des pratiques de récupération après sinistre

Gestion des Données CockroachDB

Présent dans : environnement autonome

CockroachDB est une base de données SQL distribuée et conçue à l'échelle mondiale, avec une haute disponibilité et une forte cohérence. CockroachBD offre résilience et haute disponibilité pour les applications critiques en tant que service entièrement géré encapsulé dans l'instance Corti du client.

La base de données CockroachDB offre :

- Une disponibilité maximisée en utilisant des techniques de réplication des données
- Une haute disponibilité lorsqu'elle est configurée comme solution distribuée Une récupération automatique des pannes d'hébergement au niveau du
- disque, de la machine, du rack ou du centre de données Une mise à l'échelle et une réparation automatiques
- Prend en charge la sauvegarde des informations importantes dans le cadre
- des pratiques de récupération d'incidents et de continuité des activités

Elasticsearch

Présent dans : environnement autonome

Corti fournit aux clients de sa solution des fonctionnalités de recherche élastique pour les aider à maximiser l'extraction d'informations des bases de données, améliorant ainsi la visibilité de l'infrastructure et des données pour fournir des insights et des visualisations.

- Capacités de recherche et d'analyse de données haute performance
- Fonctionnalité d'observabilité pour la surveillance de la santé de l'infrastructure et l'analyse des performances en temps réel
- Fournit des fonctions avancées de prévention, de détection et de réponse aux menaces pour soutenir la protection des points de terminaison, la gestion des événements et la chasse active aux menaces

Principes de Protection des Données

Nous reconnaissons l'importance de la sécurité pour protéger les informations sensibles de santé, c'est pourquoi la protection des données sous-tend chaque aspect de nos opérations commerciales.

Politique de Sécurité de l'Information

Corti s'engage pleinement à protéger toutes les informations sensibles des patients. Nous reconnaissons que tous nos employés sont responsables de la sauvegarde et de la protection de ces informations, qui sont essentielles au succès des opérations commerciales. En conséquence, nous veillons à ce que notre personnel et nos produits soient adéquatement protégés et restent conscients que nos activités commerciales sont d'un intérêt et d'une valeur potentiels. Les menaces incluent nos concurrents ou les parties qui pourraient chercher à voler ces informations, à nuire à notre réputation ou à perturber nos opérations.

En tant que CTO de Corti, responsable de la sécurité de l'information, je m' engage à mettre en œuvre cette politique de sécurité de l'information là où elle s'applique à l'entreprise. De plus, je la conseillerai et la soutiendrai pour en assurer la promotion active et la réalisation de sa pleine conformité.
Cet engagement est une extension naturelle et vitale des obligations de gouvernance d'entreprise et de gestion des risques de l'entreprise.

IA Responsable chez Corti

Aperçu des Stratégies et Efforts pour atténuer les risques de l'IA dans une Entreprise

L'adoption de l'intelligence artificielle (IA) dans les opérations commerciales apporte de nombreux avantages, mais elle introduit également des risques importants, notamment les biais, les préoccupations en matière de confidentialité des données, les vulnérabilités de sécurité et les conséquences imprévues. Des stratégies efficaces d'atténuation des risques sont essentielles pour garantir que le déploiement de l'IA est éthique, sûr et aligné avec les objectifs des cas d'utilisation concrets et les valeurs sociétales dans la poursuite de résultats bénéfiques pour les personnes.

Aperçu
de la Sécurité et
de la Gouvernance
de Corti

Bien que l'avènement des outils d'IA générative sophistiqués ait attiré davantage l'attention sur les risques de l'IA, ces risques ne sont pas nouveaux. Et ils ne sont pas nouveaux pour nous. Chez Corti, nous nous engageons à construire et déployer des technologies d'IA de manière responsable, tout en nous concentrant en permanence sur les considérations éthiques et le bien-être de ceux qui en ont besoin.

Voici les différentes stratégies et efforts concrets que Corti prend pour atténuer les risques de l'IA.

Cadres de Gouvernance Robustes

Comités d'éthique de l'IA :
Corti a formé des comités d'éthique de l'IA interdisciplinaires composés de data scientists, d'éthiciens, d'experts juridiques et de dirigeants d'entreprise et met en œuvre des examens réguliers des projets d'IA pour garantir qu'ils respectent les normes éthiques et les exigences réglementaires.

Politiques et directives claires :
Corti a développé des politiques et directives internes complètes qui définissent les pratiques acceptables de l'IA, l'utilisation des données et les processus de prise de décision et veille à ce que ces directives soient alignées avec les normes légales et éthiques.

Mécanismes de responsabilité :
Corti attribue une responsabilité claire pour les résultats des systèmes d'IA et met en œuvre des audits réguliers et des évaluations d'impact pour surveiller les performances des systèmes d'IA et identifier les risques potentiels tôt.

Humains aux commandes :
Corti a développé ses produits en veillant à ce que les décisions soient prises par des humains.

Transparence et Explicabilité

Modèles explicables :
Corti privilégie les modèles d'IA explicables et interprétables par rapport aux modèles de boîte noire, en particulier dans les décisions à enjeux élevés. Corti utilise des techniques telles que LIME (Local Interpretable Model-agnostic Explanations) et SHAP (SHapley Additive exPlanations) pour interpréter les décisions des modèles et effectue des recherches internes actives en IA explicable. En garantissant cela, nous permettons aux utilisateurs d'interpréter correctement les résultats du système et de
les utiliser de manière appropriée, favorisant ainsi la confiance dans nos solutions d'IA.

Développement transparent :
Corti garantit un processus de développement transparent de nos systèmes d'IA, fournissant des aperçus sur la manière qualitative dont les ensembles de données sont collectés, nettoyés et assurés, sur quelles modalités d'entrée les modèles sont entraînés, quels résultats ils produisent et quels objectifs ils sont autorisés à optimiser.

Expérience utilisateur transparente :
Corti veille à ce qu'il soit toujours transparent pour les utilisateurs lorsqu'ils interagissent avec un système d'IA et quelles suggestions, prédictions et automatisations sont faites en utilisant des modèles d'IA. Les explications des modèles et le processus de développement sont mis à disposition des utilisateurs là où cela est pertinent pour leur utilisation sûre et transparente du logiciel.

Documentation and reporting :
Corti maintient une documentation complète des processus de développement de l'IA, des ensembles de données utilisés et des justifications des décisions et produit des rapports réguliers sur les performances des systèmes d'IA, y compris des métriques sur l'équité, la précision et l'impact, pour les parties prenantes internes et externes.

Surveillance et Évaluation Continues :

Surveillance des biais :

Corti déploie des outils de détection des biais et des métriques pour surveiller en continu les systèmes d'IA en production pour les modèles discriminatoires. Corti valide régulièrement les modèles d'IA par rapport à des ensembles de données mis à jour pour garantir une équité continue. Cela inclut l'utilisation de données diverses et représentatives, des techniques de prétraitement, et des approches de traitement et de post-traitement pour ajuster les résultats des modèles et garantir l'équité.

Surveillance des performances :

Corti a établi des indicateurs clés de performance (KPI) pour les systèmes d'IA, en se concentrant sur la précision, l'équité et les considérations éthiques. Corti utilise des systèmes de surveillance automatisés pour suivre les performances de l'IA en temps réel et signaler les anomalies.

Alignement sur les valeurs humaines et l'équité :

Ces mécanismes englobent une approche globale pour prévenir l'identification injuste, le profilage ou la singularisation statistique de toute population segmentée basée sur diverses caractéristiques sensibles telles que la race, l'identité de genre, la nationalité, la religion, le handicap ou tout autre identifiant politiquement chargé. Nous croyons en la fourniture d'opportunités égales et de résultats équitables pour chaque personne touchée par nos systèmes d'IA, indépendamment de leur origine, de leur ethnie ou de toute autre caractéristique.

Confidentialité et Sécurité des Données

Sécurisé et robuste :

Corti emploie des mécanismes pour garantir la conception, le développement, les tests, la mise en œuvre et la maintenance sécurisés et résilients des systèmes d'IA. Il garantit que les systèmes d'IA restent résilients contre les erreurs, les défauts, les incohérences et les actions malveillantes qui pourraient compromettre la sécurité du système. Le système est conforme au cadre de sécurité SOC2 type 2.

Anonymisation et chiffrement des données :
Corti met en œuvre des techniques solides d'anonymisation des données pour protéger l'identité des individus dans les ensembles de données et utilise le chiffrement pour protéger les données pendant le stockage et la transmission.

Contrôles d'accès :
Corti applique des contrôles d'accès stricts pour limiter qui peut voir ou modifier des données sensibles et examine régulièrement et met à jour les autorisations d'accès pour prévenir tout accès non autorisé.

Plans de Réponse aux Incidents :
Corti a développé et maintient des plans de réponse aux incidents pour traiter rapidement les violations de données ou les défaillances des systèmes d'IA. Corti effectue également des exercices réguliers pour garantir la préparation aux incidents potentiels.

Droits à la Vie Privée :
Corti est conforme aux cadres de confidentialité RGPD et HIPAA et dispose de politiques, processus et procédures pour adhérer à leurs exigences, par exemple, fournir des droits aux utilisateurs et obtenir leur consentement. Les données sont traitées uniquement à des fins spécifiques et sur une base légale documentée avant la collecte et le traitement des données. Les données sont utilisées uniquement selon les instructions documentées. Les données ne sont jamais utilisées pour le profilage ou le marketing personnalisé, par exemple.

Une Culture d'Utilisation Éthique de l'IA

Formation et Éducation :
Corti fournit une formation continue aux employés sur l'éthique de l'IA, l'atténuation des biais et l'utilisation responsable de l'IA. Corti encourage une culture d'apprentissage continu et de sensibilisation éthique.

Engagement des Parties Prenantes :
Corti engage les parties prenantes, y compris les clients, les employés et les représentants de la communauté, pour comprendre leurs préoccupations et perspectives sur l'utilisation de l'IA.

Intègre les retours des parties prenantes dans les processus de développement et de déploiement de l'IA.

Collaboration et Normes de l'Industrie :
Corti participe à des collaborations académiques et industrielles pour partager les meilleures pratiques et rester à jour sur les dernières avancées en matière d'atténuation des risques de l'IA. Corti contribue également au développement de normes industrielles, de directives et de recherches académiques pour une utilisation responsable de l'IA.

Gouvernance

Le conseil d'administration reconnaît que les responsabilités du secteur de la santé en matière de sécurité des patients et de qualité des soins nécessitent une bonne gouvernance d'entreprise pour fonctionner légalement et éthiquement. Par conséquent, le conseil s'engage à fournir le dévouement, le soutien et la volonté nécessaires pour être tenu responsable.

Corti a établi une gouvernance organisationnelle pour orienter ses processus de prise de décision pour ses opérations commerciales. Les contrôles de gouvernance définissent les procédures et la responsabilité nécessaires pour atteindre ces objectifs dans les limites des exigences législatives, réglementaires et éthiques.

Nous nous engageons à appliquer le leadership, l'engagement et les ressources nécessaires pour une bonne gouvernance. Cette gouvernance englobe tous les aspects de l'entreprise, ses processus, sa culture et les comportements des employés. Nous veillons à ce que la gouvernance influence la planification stratégique et pilote la gestion des risques.

Certification et Accréditation

Nous reconnaissons l'importance de la certification et de l'accréditation en matière de sécurité pour démontrer la conformité aux meilleures pratiques de l'industrie pour la protection des informations sensibles de santé.

Notre Plateforme Sécurisée

La solution Corti utilise Microsoft Azure pour les services d'hébergement de données, avec la capacité d'héberger les données de chaque client dans une région géographique sélectionnée pour répondre à leurs exigences en fonction des services utilisés.

Microsoft a conçu Azure avec des contrôles de sécurité de pointe, des outils de conformité et des politiques de confidentialité pour protéger les données stockées dans le cloud. Cette fonctionnalité garantit que la plateforme de services Corti est conforme aux normes de confidentialité mondiales et régionales, y compris :

- ISO/IEC 27001 : norme internationale pour la gestion de la sécurité de l'information
- ISO/IEC 27018 : code de pratique pour la protection des informations personnellement identifiables (PII) dans les clouds publics agissant en tant que processeurs de PII
- SOC 1 : contrôles du système et de l'organisation pour les rapports financiers
- SOC 2/3 : contrôles du système et de l'organisation pour la conformité et les opérations
- US FedRAMP : programme de gestion des risques et d'autorisation fédéral pour les services cloud
- EU-U.S. Privacy Shield Framework pour le transfert de données personnelles vers les États-Unis
- EU RGPD : règlement général sur la protection des données pour la protection et la confidentialité des données personnelles au sein de l'Union européenne
- HIPAA/HITEC : loi sur la portabilité et la responsabilité en matière d'assurance maladie et Loi sur la technologie de l'information en santé économique et clinique pour la protection des informations de santé protégées (PHI) aux États-Unis

Aperçu de la Sécurité et de la Gouvernance de Corti

Azure propose des services conformes aux contrôles de sécurité pour les normes nationales, le cas échéant, y compris :

- MTCS : norme de sécurité multi-niveaux pour le cloud de Singapour pour la sécurité et la confidentialité des données dans le cloud
- IRAP : programme d'évaluateurs enregistrés en sécurité de l'information en Australie pour l'évaluation du stockage, du traitement et de l'infrastructure de communication des données
- ENS : mesures de sécurité de haut niveau espagnoles (Esquema Nacional de Seguridad) pour les services cloud
- CCPA : loi californienne sur la protection de la vie privée des consommateurs
- BSI C5 : norme de sécurité des données de santé sur le cloud de l'Allemagne
- HDS - Certification des hébergeurs de données de santé en France

Plus d'informations et de documentation sur la conformité de Microsoft Azure à de nombreuses autres normes sont disponibles ici : https://learn.microsoft.com/en-us/azure/compliance/

Aperçu
de la Sécurité et
de la Gouvernance
de Corti

Certification et Accréditation de Corti

Corti veille à ce que ses contrôles de protection des données et de cybersécurité soient alignés sur les exigences du marché et réglementaires, y compris la conformité à plusieurs cadres stricts :

- SOC2/3 - Contrôles du système et de l'organisation pour la conformité et les opérations - démontré par un audit externe de type 2.
- GDPR - Règlement général sur la protection des données pour la protection et la confidentialité des données personnelles dans l'UE et au Royaume-Uni - démontré par un audit externe ISAE 3000 de type 1.
- EU-U.S. Privacy Shield Framework pour le transfert de données personnelles vers les États-Unis, y compris le cadre de confidentialité des données Suisse-États-Unis et l'extension du Royaume-Uni. Réglementation HIPAA
- sur la confidentialité des données de santé aux États-Unis.
  US FedRAMP - Programme de gestion des risques et d'autorisation fédéral
- pour les services cloud
  Système d'information criminelle des États-Unis (CJIS) - Corti se conforme à la
- réglementation CJIS pour les produits sans accès aux dossiers criminels. BSI C5 de l'Allemagne pour la sécurité des données de santé sur le cloud -démontré
- par un audit externe de type 1.
  Certification de la norme de sécurité Cyber Essentials au Royaume-Uni.
- Certification du kit d'outils de sécurité et de protection des données (DSPT) au
- Royaume-Uni.
  Conformité au système de gestion des risques cliniques DCB0129 au
- Royaume-Uni.
  Rapport de conformité aux critères d'évaluation des technologies
- numériques (DTAC) au Royaume-Uni disponible pour les clients.

Si vous souhaitez en savoir plus sur les certifications et accréditations de Corti, visitez notre Centre de Confiance ici !