MESURES DE SÉCURITÉ MEDAVIZ

AVRIL 2024 – DIFFUSION PUBLIQUE

CERTIFICATIONS	
ISO-27001	Medaviz est certifié ISO-27-001 depuis juillet 2022. La norme ISO-27001 fournit un cadre pour un Système de Management de la Sécurité de l'Information (SMSI) qui permet le maintien de la confidentialité, de l'intégrité et de la disponibilité des informations, ainsi que la conformité légale.
HÉBERGEUR DE DONNÉES DE SANTÉ (HDS)	Medaviz est certifié HDS depuis le mois d'avril 2023 sur les piliers 1 à 5. La certification HDS valorise notre niveau de sécurité. Elle s'appuie sur la certification ISO-27001 pour répondre aux enjeux de sécurité des données et est agrémentée d'exigences additionnelles en lien avec le Règlement Général sur la Protection des Données personnelles (RGPD) et le domaine de la santé. La sécurité des données porte sur les mesures prises afin de protéger les données de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées, ainsi que l'accès non autorisé à de telles données, de manière accidentelle ou illicite.
PERSONNES	
CONFIDENTIALITÉ	Tous les employés signent un accord de confidentialité avant de commencer à travailler pour Medaviz.
FORMATION	Alors que nous ne gardons qu'une quantité minimale de données client et que nous limitons l'accès interne selon la nécessité, tous les employés sont formés à la sécurité et la gestion des données pour faire en sorte qu'ils soient attachés à notre engagement strict de la confidentialité et la sécurité de vos données.
GESTION DES PERSONNELS	Tous les employés de Medaviz passent par une vérification approfondie de leur profil avant leur embauche.
FIABILITÉ ET REDONDANCE	
CONTINUITÉ BUSINESS ET RÉCUPÉRATION APRÈS SINISTRE	Nous avons un Plan de Continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA) après sinistre qui répliquent notre base de données et sauvegardent les données chez plusieurs fournisseurs de cloud pour assurer leur haute disponibilité.
SÉCURITÉ ACTIVE	
CHIFFREMENT DES DONNÉES	Le chiffrement d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines. Medaviz utilise un chiffrement symétrique des données (permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée clé secrète.)

	cf. Sécurisation de l'exploitation
CLOISONNEMENT	Afin de réduire la possibilité de corréler des données à caractère personnel et de provoquer une violation de l'ensemble des données, Medaviz a découpé son environnement à la manière d'un puzzle, sans impact sur les tables et les données utilisateurs. Le cloisonnement système limite les conséquences d'une corruption ; les données de santé, les rendez-vous, les documents, etc. sont accessibles uniquement par les personnes ayants droit ; la compromission d'une sous-partie devient plus difficile car sa surface d'attaque est réduite.
CONTRÔLE DES ACCÈS LOGIQUES	Les profils utilisateurs sont définis en fonction des droits d'accès aux données personnelles. 3 niveaux sont définis : — Accès limité : patient (édition et consultation de ses données), secrétaire (selon autorisation de la délégation) — Accès étendu : professionnel de santé + admin (édition et consultation de ses données + données patients) — Accès total : superAdmin Une revue annuelle des habilitations est réalisée afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.
GESTION DES POSTES DE TRAVAIL	— Inventaire et mise à jour des logiciels et matériels, — Antivirus sur les postes des collaborateurs, — Mot de passe de session, — Double authentification Google et Medaviz, — Accès physique au matériel limité.
JOURNALISATION	Des logs d'accès au serveur anonymisés permettent : — d'historiser l'utilisation de la plateforme, — d'identifier un accès frauduleux, une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, — d'établir des statistiques à usage interne, — d'établir des statistiques anonymes et génériques vers l'extérieur.
SAUVEGARDE DES DONNÉES	Serveur principal à Paris (FR) avec sauvegarde quotidienne (tampon de 30 jours) et réplication sur un autre site géographique (Francfort – DE). L'infrastructure physique de Medaviz est hébergée et gérée au sein des centres de données sécurisées d'Amazon, qui réalise cette prestation uniquement sur le sol Européen. Medaviz s'appuie sur l'ensemble des fonctionnalités intégrées de sécurité, de confidentialité et de redondance de la plate-forme. AWS surveille continuellement ses centres de données et est soumis à des évaluations afin de s'assurer du respect de normes de l'industrie. Les opérations de centre de données d'Amazon ont été accréditées selon : ISO 27001, SOC 1 et SOC 2/SSAE 16/ISAE 3402 (autrefois SAS 70 Type II), PCI niveau 1, FISMA modérée et Sarbanes-Oxley (SOX). Présentée par l'Agence du Numérique en Santé (ANS) la certification Hébergeur de Données de Santé (HDS) a pour objectif de renforcer la sécurité et la protection des données personnelles de santé. AWS est certifié HDS et garantit la confidentialité, l'intégrité et la disponibilité des données personnelles de santé à ses clients et partenaires.
SÉCURISATION DE L'EXPLOITATION	SÉCURITÉ PASSIVE La plateforme Medaviz est une solution logiciel SaaS hébergée, qui est de ce fait, par design, complètement découplée, indépendante et fermée. Le seul port de communication exposé entre le client (app mobile pour le patient ou interface

	web pour le professionnel de santé) et la plateforme Medaviz, est le port 443 (https) aux travers duquel transitent les informations cryptées par un certificat SSL (chiffrement RSA). Les médias (audio/vidéo) échangés entre professionnels de santé et patients lors d'une téléconsultation sont également chiffrés de bout en bout. Ces échanges de données sont basés sur les protocoles de sécurité WebRTC et sont directs (de pair-a-pair) sans intermédiaire. Cette architecture permet de réduire au maximum la surface d'attaque. Le service ssh, protégé par clé privée et permettant à Medaviz d'administrer et de mettre à jour les systèmes, est également protégé par un pare-feu (filtrage IP, seuls les locaux de Vannes sont autorisés). Il est exclusivement accessible au travers d'un vpn et d'un bastion (enregistreur d'activité) fournis et maintenus par notre hébergeur AWS, dans le cadre d'un hébergement certifié HDS, réduisant ainsi encore une fois, la surface d'attaque. A ce jour, seules deux personnes (Directeur technique et directeur des développements Medaviz) sont habilitées et autorisées à se connecter à l'infrastructure de production. SÉCURITÉ ACTIVE La plateforme Medaviz est pourvue d'un système de monitoring de code et de performance, en plus des logs d'activité habituels. Des alertes avertissent les équipes en cas d'activité anormale (ex : brute force) ou de dépassement de seuils (ex : dépassement du seuil de 800 requêtes seconde sur une ressource, indiquant une activité non humaine). SÉCURITÉ DES FICHIERS Les fichiers produits sur la plateforme Medaviz (ordonnances générées en pdf par exemple) sont des fichiers stockés dans une base de données S3. Ainsi ils ne sont pas exposés de manière classique, dans un système de fichiers classique, qui pourrait rendre la lecture de ces derniers simples. Cette base de données est également sauvegardée de manière quotidienne sur l'infrastructure HDS. Les données dites relationnelles sont dans une base de données MariaDB. Cette base héberge les données utilisateurs, avec notamment les mots de passe de ces derniers, cryptés en SHA-256. Cette base est également sauvegardée de manière quotidienne sur l'infrastructure HDS. Le reste des fichiers sont des fichiers dit de codes, ne contenant aucune information personnelle. Il est également à noter que les couples identifiant/mot de passe (sensibles) de connexion aux bases de données, exploitées par le code afin de faire fonctionner la plateforme, sont gérés par un système de secrets. L'objectif : ne pas divulguer ces informations dans de simples fichiers de configuration ou dans un référentiel de code, accessibles si l'infrastructure se retrouvait corrompue, ou par des développeurs non habilités. SÉCURITÉ INTERNE Medaviz est une plateforme entièrement scriptée (logiciel et infrastructure) et dockerisée. Les services (email, push, base de données) sont dans des conteneurs, scalables, et déployables à souhait. Cette technologie nous permet de redéployer la plateforme dans un temps record, en réaction à une attaque par exemple, après avoir isolé la faille de sécurité. Elle assure également la capacité de la solution à supporter des volumes d'usages exceptionnels. cf. Recherche de vulnérabilité
SÉCURISATION DES CANAUX INFORMATIQUES	La sécurité est un point d'attention de chaque instant pour nous. Plusieurs points ont été mis en place à ce sujet : D'UN POINT DE VUE MATÉRIEL — Hébergement HDS chez AWS. — Infrastructure derrière un firewall. — Accès système au travers d'un VPC et surveillés par un bastion (enregistrement de toutes les actions d'administration).

	D'UN POINT DE VUE LOGIQUE — Accès à la plateforme Medaviz qui requiert une authentification à double facteur : n° de mobile-mot de passe + OTP. — Mots de passe cryptés en sha256. — Séquences d'authentification protégées CSRF. — Échanges vidéos via le module twilio en peer-to-peer et cryptés de bout en bout (pas de serveur central). — Logique de rôle, avec niveaux d'accès différents / ajustés d'un rôle à l'autre. — Back-up quotidien. cf. Sécurisation de l'exploitation
SÉCURISATION DES MATÉRIELS	cf. Lutte contre les logiciels malveillants
TRAÇABILITÉ	La plateforme Medaviz est pourvue d'un système de monitoring de code et de performance, en plus des logs d'activité habituels. Des alertes avertissent les équipes en cas d'activité anormale (ex : brute force) ou de dépassement de seuils (ex : dépassement du seuil de 800 requêtes seconde sur une ressource, indiquant une activité non humaine).
VERSIONNEMENT DES ENTITÉES SENSIBLES	Le versionnement des entités consiste à surveiller et enregistrer les changements de certaines propriétés de la base de données. Ce versionnement vise à se conformer avec l'exigence HDS 4.4.6.10 : "L'hébergeur doit mettre en œuvre les moyens d'assurer la traçabilité des actions des utilisateurs, des défaillances et des événements liés à la sécurité de l'information. Les journaux contenant les traces doivent être conservés et revus régulièrement. L'hébergeur doit assurer l'intégrité des journaux et les protéger des accès illicites." En l'occurrence, le versionnement des entités de la base de données de my.medaviz.io s'effectue dans 3 cas : création, modification et suppression d'une donnée.
CYCLE DE DÉVELOPPEMENT APPLICATIF	
ANONYMISATION DES DONNÉES	Pour des raisons de confidentialité, les collaborateurs Medaviz utilisent l'ID utilisateur si besoin d'intervenir sur des comptes utilisateurs. Le script d'archivage anonymise toutes les données personnelles de l'utilisateur.
ARCHIVAGE	DONNÉES PERSONNELLES Lorsqu'un utilisateur demande la suppression de son compte, Medaviz conserve certaines des données personnelles afin de satisfaire aux obligations légales, comptables et fiscales (délai de conservation de 10 ans) et de pouvoir exercer ses droits en justice pendant le délai de prescription applicable (délai de prescription de droit commun de 5 ans). DOCUMENTS Archivage intermédiaire (24 mois) des documents générés lors d'actes de télémédecine (sous-traitant) pour des raisons de sécurité ISO-270001/ RGPD (minimiser les données sensibles en cas d'intrusion), et de stockage. Toutes les données de santé sont sous la responsabilité des praticiens. Les archives sont sécurisées (serveur HDS).
CONTRAT DE SOUS-TRAITANCE	Les sous-traitants garantissent la maintenance régulière des équipements ainsi que la fourniture électrique redondée et la climatisation de la salle serveurs.

	Nous veillons au maximum que les données personnelles restent dans l'Union européenne en révisant régulièrement les contrats. Si les données sont transférées hors Union européenne, nous demandons les garanties équivalentes pour assurer la confidentialité, l'intégrité et la disponibilité des données.
INTÉGRATION DE LA PROTECTION DE LA VIE PRIVÉE DANS LES PROJETS	À chaque étape de la conception produit Privacy by Design, Medaviz veille au respect de la conformité en suivant les recommandations CNIL. La conformité RGPD est documentée et mise à jour en continue par le DPO qui est également le Responsable produit.
MINIMISATION DES DONNÉES	À chaque étape de la conception produit Privacy by Design, Medaviz : — minimise la collecte des données (strictement nécessaire), — évite toute accumulation inutile, — restreint l'accès aux données avec le contrôle des accès logiques.
NOUVELLES VERSIONS	Les nouvelles versions de la plate-forme Medaviz sont soigneusement examinées et testées pour garantir une disponibilité élevée et une expérience client exceptionnelle. Les modifications apportées à notre base de code sont tenues d'inclure des tests unitaires, des tests d'intégration et des tests de bout en bout. Les modifications sont exécutées sur notre serveur d'intégration continue, qui nous permet de détecter automatiquement tous les problèmes de développement.
TESTS D'ASSURANCE QUALITÉ	Une fois qu'un ensemble de modifications est terminé, il est manuellement revu par un ou plusieurs membres de l'équipe d'ingénierie. L'ensemble de modifications est alors évalué et testé manuellement par notre équipe d'assurance qualité pour tester en profondeur les zones d'impact attendu, de régression et pour continuer à évaluer l'expérience de l'utilisateur.
CONTRÔLE DE VULNÉRABILITÉ	
RECHERCHE DE VULNÉRABILITÉ	Des tests de sécurité interne sont conduits tous les mois, avec comme support la base de données des vulnérabilités php, afin de détecter et corriger de potentielles failles de sécurité (injection sql, attaque csrf, packages vulnérables, etc.). En parallèle, des revues de code hebdomadaires sont conduites par les équipes de développement (pair programming), et ont pour but d'améliorer la qualité du code en termes de performance et sécurité.
GESTION DES INCIDENTS DE SÉCURITÉ ET DES VIOLATIONS DE DONNÉES	Les incidents sont référencés dans un registre des violations et incidents avec déclaration à la CNIL. Communication réactive auprès de nos utilisateurs le cas échéant.
GESTION DES RISQUES	Chaque année, un audit technique de la plateforme est mené par un prestataire qualifié PASSI par l'Agence Nationale de la Sécurité des Systèmes d'informations. Cet audit technique comprend un test d'intrusion sur l'applicatif Medaviz. Attestation de test d'intrusion_202306_Medaviz_Own.pdf.pdf cf. Traçabilité + cf. Sécurisation de l'exploitation
LUTTE CONTRE LES LOGICIELS MALVEILLANTS	Nous sécurisons les machines et ordinateurs portables de nos employés grâce à la gestion de terminaux mobiles pour nous assurer que chaque appareil est conforme à nos normes de sécurité de l'information, y compris le cryptage.

	Les équipements de nos employés sont protégés par des logiciels anti-malware, et nous exécutons des tests de routine de hameçonnage (phishing) pour éduquer et former nos employés. cf. Sécurisation de l'exploitation
PROTECTION DES SITES WEB	cf. Sécurisation de l'exploitation
RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES	
GESTION DE LA POLITIQUE DE PROTECTION DE LA VIE PRIVÉE	Un dossier RGPD est partagé aux collaborateurs de Medaviz afin de suivre l'intégralité de la conformité. Le DPO et la juriste s'assurent de : — Documenter la conformité (les mesures organisationnelles et techniques sont ré-examinées et actualisées) — Gérer les risques (démontrer que les principes fondamentaux du règlement sont respectés). — Organiser les processus internes (faille de sécurité, gestion des droits des personnes, changement de prestataire, etc).
ORGANISATION DE LA POLITIQUE DE PROTECTION DE LA VIE PRIVÉE	— Délégué à la Protection des Données déclaré à la CNIL le 23/06/2021. — Profil du DPO : Responsable produit — Points hebdomadaire avec une juriste pour suivre la conformité Points hebdo — Points semestriels avec la direction et le Responsable de Traitement pour rendre compte de la conformité RGPD.
SUPERVISION DE LA PROTECTION DE LA VIE PRIVÉE	La protection de la vie privée est suivie par le DPO, garant de la mise en conformité en matière de protection des données. — Informe et conseille l'entreprise et ses employés. — Instaure les moyens et actions à mettre en place en conformité avec la réglementation. — Veille au respect et au maintien de la conformité, notamment la documentation. — Contrôle la conformité au règlement, avec l'expertise du juriste.