Politique de divulgation coordonnée des vulnérabilités

Objectif et engagement

Dans le cadre de ses activités, EMA conçoit et exploite des solutions numériques susceptibles de traiter des données sensibles, notamment des données de santé, ou de contribuer à des fonctions critiques liées à la prise en charge des patients.

La sécurité de ces solutions constitue une priorité essentielle. À ce titre, EMA s'engage à maintenir un niveau élevé de protection contre les risques de cybersécurité susceptibles d'affecter :

- la confidentialité des données de santé
- l'intégrité des informations médicales
- la disponibilité des services nécessaires à la continuité des soins

La présente politique a pour objectif de définir un cadre clair, transparent et responsable permettant à toute personne externe d'identifier et de signaler des vulnérabilités de sécurité.

Elle vise également à garantir que ces vulnérabilités sont traitées de manière rigoureuse, coordonnée et proportionnée à leur impact potentiel, conformément aux exigences réglementaires applicables.

Périmètre d'application

Cette politique s'applique à l'ensemble des produits et services numériques développés, maintenus ou exploités par EMA, incluant notamment :

- les logiciels et applications (y compris les dispositifs médicaux logiciels le cas échéant)
- les plateformes de gestion de données de santé
- les interfaces utilisateurs accessibles aux professionnels de santé ou aux patients
- les services en ligne et infrastructures associées

Certains environnements, notamment ceux critiques pour la sécurité des patients ou la continuité des soins, peuvent être exclus de toute activité de test active. Ces restrictions visent à éviter toute perturbation des services essentiels.

Lorsque des limitations spécifiques existent, elles sont précisées dans les supports d'information mis à disposition des utilisateurs.

Modalités de signalement

Toute personne identifiant une vulnérabilité de sécurité est invitée à la signaler via le point de contact dédié : security@hemadialyse.com

Afin de permettre une analyse efficace, le signalement doit inclure autant d'informations que possible, notamment :

- une description détaillée de la vulnérabilité
- les conditions nécessaires à sa reproduction
- l'environnement concerné (version, configuration, contexte d'usage)
- une estimation de l'impact potentiel, en particulier sur les données ou les fonctions critiques
- tout élément technique utile (preuves de concept, journaux, captures d'écran, etc.)

Les données personnelles présentent dans ce signalement doivent être limitées au minimum.

Engagement de l'organisation

EMA s'engage à traiter tout signalement de manière professionnelle et responsable.

À ce titre, elle s'engage à :

- accuser réception du signalement dans un délai raisonnable
- analyser la validité et l'impact de la vulnérabilité
- maintenir un dialogue approprié avec le déclarant lorsque cela est possible
- mettre en œuvre des mesures correctives ou compensatoires adaptées
- prioriser le traitement en fonction du niveau de risque, notamment lorsque des fonctions critiques ou des données sensibles sont concernées

Lorsque le déclarant le souhaite, sa contribution peut être reconnue, sous réserve du respect des règles de divulgation coordonnée.

Attentes vis-à-vis des déclarants

Afin de garantir la sécurité des systèmes et des utilisateurs, en particulier dans un contexte de santé, les déclarants sont invités à adopter un comportement responsable.

Il leur est notamment demandé de :

- agir de bonne foi et dans le respect des lois et réglementations applicables
- éviter toute action susceptible d'impacter la sécurité des patients ou la continuité des soins
- ne pas accéder, modifier ou supprimer des données réelles, en particulier des données de santé
- limiter les tests au strict nécessaire pour démontrer l'existence de la vulnérabilité
- ne pas divulguer publiquement les informations relatives à la vulnérabilité avant qu'une solution n'ait été mise en œuvre ou qu'un accord explicite ait été établi

Traitement des vulnérabilités

Les vulnérabilités signalées font l'objet d'un processus structuré de gestion interne, incluant :

- une phase de validation permettant de confirmer leur existence
- une analyse de leur impact potentiel sur la sécurité, la confidentialité et la continuité des services
- une priorisation en fonction du niveau de risque, en tenant compte notamment des impacts sur les patients et les professionnels de santé
- la mise en œuvre de mesures correctives ou de mesures d'atténuation appropriées

Une attention particulière est portée aux vulnérabilités susceptibles d'affecter des fonctions essentielles, des dispositifs médicaux logiciels ou des données de santé.

Le traitement est réalisé conformément aux processus internes de gestion des risques et des incidents de sécurité.

Divulgation coordonnée

EMA applique un principe de divulgation coordonnée des vulnérabilités.

Cela implique que :

- les informations relatives à une vulnérabilité ne sont rendues publiques qu'après la mise en place de mesures correctives ou de mesures d'atténuation appropriées
- la publication peut être réalisée en coordination avec le déclarant lorsque cela est possible
- les modalités de divulgation tiennent compte des enjeux de sécurité, en particulier dans le contexte de la santé

Information des utilisateurs

Lorsque cela est nécessaire, notamment en cas de risque pour les utilisateurs ou les patients, l'organisation peut communiquer des informations relatives à une vulnérabilité ou à un incident de sécurité.

Ces communications peuvent prendre la forme :

- d'avis de sécurité
- de mises à jour logicielles
- de recommandations d'usage

L'objectif est de permettre aux utilisateurs de prendre les mesures appropriées pour maintenir un niveau de sécurité adéquat.

Conformité réglementaire

EMA se conforme aux exigences réglementaires applicables en matière de cybersécurité, en particulier celles relatives aux produits numériques et aux systèmes traitant des données sensibles.

Dans ce cadre, certaines vulnérabilités ou incidents de sécurité peuvent faire l'objet de notifications auprès des autorités compétentes, conformément aux obligations légales en vigueur.

Articulation avec la gestion des incidents

Les vulnérabilités signalées dans le cadre de cette politique sont traitées selon leur nature et leur niveau de criticité.

Lorsqu'une vulnérabilité est susceptible d'être exploitée activement ou de donner lieu à un incident de sécurité, elle est prise en charge dans le cadre des processus internes de gestion des incidents de cybersécurité.

Ces processus visent notamment à :

- limiter l'impact potentiel sur les systèmes et les données
- assurer la continuité des services
- protéger les utilisateurs et les patients

Amélioration continue

L'organisation s'inscrit dans une démarche d'amélioration continue de la sécurité de ses produits et services.

À ce titre :

- la présente politique est revue périodiquement
- les retours d'expérience issus du traitement des vulnérabilités sont pris en compte
- les processus internes sont ajustés en fonction des évolutions technologiques, réglementaires et des menaces
-

Contact

Pour toute question relative à cette politique ou pour signaler une vulnérabilité : security@hemadialyse.com