FMH
FÉDÉRATION MONDIALE DE L'HÉMOPHILIE
WORLD FEDERATION OF HEMOPHILIA
FEDERACIÓN MUNDIAL DE HEMOFILIA

RMTC
Registre mondial des troubles de la coagulation de la FMH

Registre mondial des troubles de la coagulation

Sécurité et confidentialité des données

Qu'est-ce que le Registre mondial des troubles de la coagulation (RMTC) ?

Le RMTC est un registre de patients dématérialisé et accessible sur Internet. Les patients sont recrutés par l'intermédiaire de centres de traitements de l'hémophilie (CTH) sélectionnés par la FMH dans le monde entier. Le système sur lequel repose le RMTC implique la mise en place d'un certain nombre de mesures visant à garantir la sécurité et la confidentialité des données recueillies et à réduire l'utilisation et la conservation d'informations pouvant permettre l'identification des patients. En conséquence, les données collectées par chaque CTH restent séparées et le RMTC ne conserve aucun moyen de les identifier directement. Il est impossible de lier les données d'un CTH à l'autre sans l'autorisation préalable du RMTC et la mise en œuvre d'un Accord de partage des données, afin de veiller à préserver la sécurité et la confidentialité des données.

Propriété des données

Les patients participant au RMTC sont recrutés par l'intermédiaire des CTH. Les données collectées auprès des patients ne le sont qu'après avoir obtenu leur consentement lors de chaque consultation. Les données des patients sont conservées de façon séparée pour chaque CTH qui n'a accès qu'aux données des patients qu'il suit. Par défaut, le CTH ne peut avoir accès aux données des patients suivis dans un autre CTH. Seul le Comité de pilotage du RMTC de la FMH peut autoriser l'agrégation de données de différents CTH.

Sécurité des données

Le RMTC utilise des systèmes de saisie des données qui préservent leur confidentialité. Ils déterminent si ladite saisie réalisée par les centres de traitement de l'hémophilie (CTH) participant au RMTC renvoie bien à une même personne, avec un niveau de précision extrêmement élevé.

Le hachage cryptographique est la technologie employée pour réduire les probabilités d'identifier un patient dans le RMTC, tout en garantissant un lien robuste. Plus précisément, l'algorithme utilisé pour hacher les informations est le SHA-26, qui est appliqué, comme cela est décrit ci-dessous, sur un ensemble précis et immuable de propriétés relatives à chaque patient.

Cet algorithme dispose d'une fonction unilatérale qui produit le même résultat s'il reçoit la même information de départ, tout en garantissant l'impossibilité informatique de tirer des conclusions sur les données fournies au départ (à savoir à partir des données permettant d'identifier chaque patient) en fonction des données finales obtenues après hachage.

En outre, une séquence aléatoire de caractères, appelée « sel », est ajoutée aux propriétés immuables du patient avant le hachage. Si d'aventure les mesures de protection des données mises en place dans le cadre du RMTC étaient contournées, cette technique du « salage » protègerait les données en luttant contre les attaques par dictionnaire visant à inférer les propriétés immuables de certains patients présentant des valeurs communes. En d'autres termes, le RMTC est adapté pour faire face à de telles attaques visant à compromettre les données qu'il renferme.

Pour bien comprendre le processus détaillé qui a été mis en place, il convient de savoir que, pour chaque

patient, les mesures suivantes ont été prises :

- Le CTH demande l'autorisation au patient de l'inclure dans le registre international, selon des procédures standards mises en place dans un système conforme au cadre réglementaire pertinent.
- Pour chaque patient, le CTH recueille les informations suivantes : date de naissance, prénom et nom, pays de naissance.
    - Ces données sont saisies dans le RMTC, mais le RMTC ne les conserve pas dans la base de données.
    - Le RMTC lance le hachage cryptographique des données du patient, qui débouche sur une ou plusieurs valeurs cryptographiques.
    - Le RMTC élimine immédiatement et de façon sécurisée les données du patient utilisées pour générer les valeurs hachées.
    - Le RMTC vérifie alors que les valeurs hachées correspondent bien à celles présentes dans n'importe quel dossier de patient, ce qui indiquerait que la personne concernée a bien été enregistrée dans le RMTC par le passé. Dans ce cas, le système va chercher le dossier correspondant. Si tel n'est pas le cas, le RMTC crée un nouveau dossier pour le patient concerné et y enregistre les valeurs hachées.
    - Quoi qu'il en soit, le RMTC attribue un nouvel identifiant de façon aléatoire au patient correspondant au CTH saisissant les informations et renvoie l'identifiant au CTH concerné.
    - Le CTH attribue l'identifiant reçu du RMTC aux données du patient concerné.

Comment le RMTC assure-t-il la sécurité et la confidentialité des données ?

Bien qu'il n'existe pas de système capable d'éliminer tout risque d'utilisation malveillante, le RMTC a été conçu et mis en œuvre pour réduire de tels risques s'agissant des données des patients. Il vise également à réduire les risques de préjudice potentiel résultant d'une éventuelle intrusion ou faille dans les mesures de protection mises en place.

Les mesures de protection intégrées au système sont notamment les suivantes :

- Le système du RMTC a été conçu et est hébergé par Health Solutions AB, un prestataire suédois spécialisé dans les technologies de l'information appliquées au domaine de la santé, dont les services sont conformes aux normes les plus strictes en termes de sécurité et de protection des données :
    - La solution RealQ, qui soutient le RMTC, est agréée par les autorités de régulation suédoise des dispositifs médicaux chargées d'appliquer la certification européenne CE aux dispositifs médicaux (Directive 93/42/EEC).
    - Ses pratiques de traitement des informations personnelles ont obtenu un agrément et sont conformes à la réglementation britannique en la matière (Information Governance Toolkit standard).
    - Les hôpitaux suédois utilisent ses services pour traiter et conserver les données médicales.
- Toute communication entre le RMTC et un CTH est réalisée par une connexion sécurisée et chiffrée d'un bout à l'autre, utilisant le protocole SSL (HTTPS), qui empêche toute tierce partie d'intercepter les échanges.

- Il est impossible à tout CTH participant d'utiliser les identifiants du RMTC pour associer les données d'un patient à un autre projet sans l'assistance et l'aval du RMTC lui-même. En effet, chaque identifiant est spécifique à chaque CTH et il n'existe donc aucun lien intrinsèque entre chaque CTH.
- Il est par conséquent impossible pour quiconque parvenant à accéder sans autorisation aux données d'un CTH participant de se connecter sans autorisation aux données figurant dans le référentiel du RMTC, qui est géré et administré de façon séparée.
- Dans la mesure où les données médicales personnelles utilisées pour générer des valeurs hachées ne sont pas sauvegardées, le système réduit les risques d'identification des patients, quand bien même une personne parviendrait malgré tout à accéder sans autorisation au référentiel des données du RMTC. Le RMTC met en œuvre des dispositifs de sécurité supplémentaires faisant appel à la méthode du salage qui applique un algorithme de hachage, non pas uniquement à chaque donnée prise individuellement, mais aussi à des séquences de données saisies. De telles mesures réduisent de façon notable le risque d'attaques de réidentification par dictionnaire.
- L'accès à la base de données du RMTC est strictement réservé aux utilisateurs ayant physiquement un accès direct aux locaux dans lesquels les serveurs sont hébergés ou ayant une connexion VPN mise en place par Health Solutions.