Registre mondial des troubles de la coagulation

Confidentialité et sécurité des données

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

Le RMTC est un registre de patients centralisé sur une base de données en ligne. Les patients sont inscrits via un réseau de centres de traitement de l'hémophilie (CTH) répartis dans le monde entier. La plateforme du RMTC intègre de nombreuses mesures de protection de la vie privée et de sécurité et réduit au minimum l'utilisation et la conservation des données d'identification. Les données provenant de chaque centre de traitement de l'hémophilie restent séparées et le RMTC ne détient aucun identifiant direct. Il est possible de partager des données entre différents CTH mais cela nécessite l'approbation préalable de la FMH et un accord *ad hoc* afin de garantir la mise en place de mesures appropriées de sécurité et de protection de la vie privée.

Propriété des données

L'inscription des patients au RMTC se fait par l'intermédiaire de leur CTH. Les données des patients ayant donné leur consentement sont saisies prospectivement dans le RMTC après chaque consultation. Les données des patients de chaque centre de soins sont conservées séparément. Chaque centre a accès aux données qu'il a lui-même collectées, mais n'a par défaut aucun accès aux données collectées par un autre centre. Il est possible d'agréger des ensembles de données entre les CTH, à condition d'obtenir l'approbation du Comité de pilotage du RMTC de la FMH et des CTH intéressés.

Sécurité des données

Le RMTC utilise un couplage d'enregistrements préservant la vie privée pour déterminer si les enregistrements des CTH participants se réfèrent à la même personne, avec un degré élevé de précision.

Le hachage cryptographique est la technologie sous-jacente qui permet au RMTC de réduire les possibilités d'identifier des patients tout en permettant un couplage solide. L'algorithme de hachage spécifique utilisé est le SHA-256, qui est appliqué à un ensemble de propriétés immuables liées à chaque patient, comme décrit ci-dessous.

Cet algorithme fournit une fonction à sens unique qui produit de manière fiable le même résultat chaque fois que la même entrée est saisie, tout en garantissant qu'il est impossible, d'un point de vue informatique, de tirer des conclusions sur les données d'entrée (à savoir les données d'identification de chaque patient) en se basant uniquement sur le résultat du hachage.

En outre, une chaîne aléatoire de caractères appelée « sel » est ajoutée aux propriétés immuables du patient avant le hachage. Dans le cas improbable où les mesures de protection mises en place par le RMTC pour empêcher tout accès non autorisé seraient contournées, cette technique de « salage » protège davantage les données en empêchant l'utilisation d'un vaste dictionnaire de valeurs de hachage précalculées pour tenter de déduire les propriétés immuables de certains patients dont les valeurs sont particulièrement communes. En d'autres termes, le RMTC reste protégé quels que soient les efforts visant à compromettre ses données.

Pour expliquer le processus plus en détail, les étapes suivantes sont suivies pour chaque patient qu'un CTH enregistre dans le système :

- Pour être inclus dans le registre international et conformément aux législations pertinentes, le CTH demande le consentement spécifique du patient.
- Le CTH recueille la date de naissance, le prénom à la naissance, le nom de famille à la naissance et le pays de naissance du patient.
    - Ces données sont saisies dans le RMTC mais ne sont pas stockées dans sa base de données.
    - Le RMTC applique plutôt une fonction de hachage cryptographique aux données patient, ce qui produit une ou plusieurs valeurs de hachage cryptographique.
    - Le RMTC élimine immédiatement et en toute sécurité les informations sur le patient qui ont été utilisées pour générer les valeurs de hachage.
    - Le RMTC vérifie ensuite si les valeurs de hachage correspondent à celles d'un dossier patient existant, ce qui indiquerait que cette personne a déjà été enregistrée dans le RMTC, et si tel est le cas, le système récupère le dossier correspondant. Si aucune correspondance n'est trouvée, le RMTC crée un nouveau dossier pour le patient et y stocke les valeurs de hachage.
    - Dans les deux cas, le RMTC attribue au patient un nouvel identifiant aléatoire spécifique au CTH et renvoie cet identifiant au CTH.
    - Le CTH attribue l'identifiant qu'elle reçoit du RMTC aux données du patient en question.

Comment le RMTC protège-t-il la vie privée et la sécurité ?

Bien qu'aucun système ne puisse éliminer complètement le risque d'utilisation abusive des données, le RMTC a été conçu et mis en œuvre de manière à minimiser le risque d'utilisation involontaire des données des patients. Il a également été conçu pour minimiser les dommages potentiels qui pourraient résulter d'une violation de telles garanties.

Les protections intégrées au système sont les suivantes :

- Le système du RMTC est conçu et hébergé par le fournisseur suédois d'informatique de santé BCB Medical, dont les services de traitement des données de santé respectent des normes strictes en matière de sécurité et de confidentialité :
    - Son produit RealQ, qui prend en charge le RMTC, est conforme à la réglementation suédoise sur les dispositifs médicaux, et applique le règlement de l'Union européenne sur le marquage CE des dispositifs médicaux, la directive 93/42/CEE, ainsi que le règlement général sur la protection des données (RGPD).
    - De telles pratiques de traitement des informations personnelles ont également été certifiées conformes à la norme *Information Governance Toolkit* du Royaume-Uni.
    - Les services de traitement des informations de santé sont utilisés par les hôpitaux suédois pour conserver et traiter les données des patients.
- Toutes les communications entre le RMTC et un CTH se font par le biais d'une connexion sécurisée qui est cryptée de bout en bout, en utilisant le protocole HTTP sur SSL (HTTPS), ce qui empêche toute tierce partie d'intercepter les communications.
- Il n'existe aucun moyen pour un CTH participant d'utiliser les identifiants du RMTC afin d'accéder aux

données des patients d'autres CTH sans la coopération et l'approbation du Comité de pilotage du RMTC. Cela est dû au fait que chaque identifiant est spécifique à un CTH et qu'ils n'ont donc aucune relation inhérente les uns avec les autres.

- Il n'existe donc aucun moyen pour quiconque accédant sans autorisation aux données d'un CTH participant d'effectuer un couplage autorisé sans avoir accès aux données du référentiel du RMTC, qui sont conservées et gérées séparément.
- Étant donné que les données de santé personnelles utilisées pour générer les valeurs de hachage ne sont pas stockées, même si une personne parvenait à obtenir un accès non autorisé au référentiel de données du RMTC, le système minimise le risque que cette personne puisse déterminer l'identité des patients conservés dans le système. Le RMTC intègre des garanties supplémentaires contre ce risque en utilisant un algorithme de hachage salé et en appliquant l'algorithme de hachage à des versions concaténées des valeurs d'entrée, plutôt qu'à chaque entrée individuelle. Ces mesures réduisent considérablement le risque d'attaques de réidentification basées sur de grands dictionnaires de valeurs de hachage précalculées.
- L'accès à la base de données du RMTC est limité aux utilisateurs ayant un accès physique aux locaux où les services sont hébergés, ou un accès à une connexion VPN établie pour BCB Medical.