Registro Mundial de trastornos de la Coagulación

Privacidad y seguridad de los datos

¿Qué es el Registro Mundial de Trastornos de la Coagulación (RMTC)?

El RMTC es un padrón de pacientes en línea, basado en Internet. Los pacientes se inscriben a través de una red mundial de centros de tratamiento de hemofilia (CTH). El sistema del RMTC cuenta con numerosas salvaguardas de privacidad y seguridad, además de reducir al mínimo el uso y la retención de información que permite identificar a los pacientes. Los datos de cada CTH permanecen separados y el RMTC no mantiene ninguna información de identificación directa. La vinculación de datos entre CTH es posible, pero requiere aprobación previa de la FMH y la firma de un acuerdo para compartir datos, a fin de garantizar que se hayan establecido salvaguardas adecuadas para proteger la seguridad y la privacidad de los mismos.

Propiedad de los datos

Los pacientes se inscriben al RMTC a través de su CTH. Los datos de los pacientes que otorgan su consentimiento se ingresan al RMTC prospectivamente, después de cada visita del paciente a la clínica. Los datos de los pacientes de cada CTH se mantienen separados. Cada CTH tiene acceso a los datos de los pacientes que ellos mismos hayan recolectado pero, de manera predeterminada, no tiene acceso a datos recolectados por otros CTH. Pueden generarse conjuntos de datos combinados de varios CTH con la aprobación del comité directivo del RMTC de la FMH y de los CTH interesados.

Seguridad de los datos

El RMTC utiliza una vinculación de registros que preserva la privacidad para determinar, con un alto grado de precisión, cuando los registros de los CTH participantes se refieren a la misma persona.

La función de dispersión criptográfica (*cryptographic hashing*) es la tecnología subyacente que permite al RMTC tanto reducir al mínimo la identificación de los pacientes, como una sólida vinculación. El algoritmo de dispersión específico que se utiliza es el SHA-256, el cual se aplica a un conjunto de propiedades inmutables relacionadas con cada paciente, como se describe a continuación.

Este algoritmo ofrece una función de sentido único que, de manera confiable, produce la misma salida siempre que recibe la misma entrada, a la vez que garantiza la imposibilidad computacional de que alguien pudiera hacer inferencias sobre los datos de entrada (i.e.: datos que identifican a cada paciente) exclusivamente a partir de la salida del *hash* por sí solo.

Además, antes del *hashing*, se agrega a las propiedades inmutables del paciente una cadena de caracteres aleatorios llamada "sal". En el poco probable caso de que pudieran burlarse las salvaguardas que el RMTC ha establecido para prevenir el acceso no autorizado a los datos, esta técnica de agregar “sal” brinda una mayor protección a los datos, evitando el uso de un enorme diccionario de valores *hash* precomputados para intentar inferir las propiedades inmutables de algunos de los pacientes con valores particularmente comunes. En otras palabras, el RMTC permanece seguro aun si se intentara este tipo de acción para comprometer sus datos.

Versión 1.1, octubre 26, 2023

A fin de explicar el proceso con más detalle, los siguientes son los pasos que se toman en el caso de cada paciente que un CTH determinado registra en el sistema:

- El CTH obtiene el consentimiento específico del paciente para ser incluido en el registro internacional, de acuerdo con los procedimientos normalizados en todo el sistema, los cuales se han establecido con apego a todas las leyes relevantes.
- El CTH recopila la fecha de nacimiento del paciente, su nombre y apellido(s) al nacer, y su país de nacimiento.
    - Estos datos se ingresan al RMTC, pero el RMTC no los almacena en su base de datos.
    - En lugar de almacenarlos, el RMTC aplica una función de dispersión criptográfica a los datos del paciente, lo que genera uno o más valores *hash* criptográficos.
    - Inmediatamente, el RMTC desecha de manera segura la información del paciente que se utilizó para generar los valores *hash*.
    - Enseguida, el RMTC verifica si los valores *hash* concuerdan con el registro de algún otro paciente, lo que indicaría que esta persona ya había sido inscrita anteriormente al RMTC y, si así fuera, el sistema recupera el registro relevante. De no encontrarse ninguna otra concordancia, el RMTC crea un nuevo registro para el paciente y almacena los valores *hash* correspondientes.
    - En cada caso, el RMTC asigna al paciente un nuevo identificador al azar, específico para el CTH que proporcionó los datos, y envía dicho identificador al CTH.
    - El CTH asigna el identificador que recibe del RMTC a los datos de ese paciente.

¿Cómo protege el RMTC la privacidad y la seguridad de los datos?

Si bien ningún sistema puede eliminar el riesgo de uso indebido, el RMTC fue concebido e implementado para minimizar el riesgo de un mal uso de los datos de los pacientes. También fue diseñado para minimizar los daños potenciales que pudieran resultar si llegaran a violarse cualesquiera de sus salvaguardas.

Las protecciones incorporadas al sistema abarcan las siguientes:

- El sistema del RMTC está diseñado y auspiciado por el proveedor de TI sueco BCB Medical, cuyos servicios de procesamiento de datos médicos se apegan a las más estrictas normas de seguridad y privacidad:
    - Su producto RealQ, que respalda al RMTC, ha sido certificado por estar registrado en cumplimiento con la reglamentación sueca para dispositivos médicos, la cual implementa el reglamento de marcado de la Unión Europea (CE) para dispositivos médicos, la Directiva 93/42/EEC, y el Reglamento General de Protección de Datos (GDPR por su sigla en inglés).
    - Sus prácticas de procesamiento de información personal también han recibido certificación de cumplimiento con la norma *Information Governance Toolkit* del Reino Unido.
    - Sus servicios de procesamiento de información médica son utilizados por hospitales suecos para almacenar y procesar datos de los pacientes.
- Todas las comunicaciones entre el RMTC y el CTH tienen lugar a través de una conexión segura, cifrada de principio a fin usando un protocolo HTTP sobre SSL (HTTPS), que evita la intercepción de cualquier comunicación entre ambos por parte de terceros.

- No hay manera de que ningún CTH participante utilice los identificadores del RMTC para vincular datos de los pacientes entre proyectos sin mediar la colaboración y aprobación del RMTC. Esto es resultado del hecho de que cada identificador es específico a los CTH, de manera que no tienen una relación inherente entre sí.
- Debido a lo anterior, no hay manera de que alguien que obtuviera acceso no autorizado a los datos de un CTH participante pudiera realizar una vinculación autorizada, sin acceso a los datos que se encuentran en el repositorio del RMTC, que se mantiene y maneja por separado.
- Dado que la información médica personal usada para generar los valores *hash* no se almacena, aun si una persona obtuviera acceso no autorizado al repositorio de datos del RMTC, el sistema minimiza el riesgo de que dicha persona pueda determinar la identidad de los pacientes cuyos datos se encuentran en el sistema. El RMTC incorpora otras salvaguardas contra este riesgo mediante el uso de un algoritmo de dispersión con "sal" y aplicando el algoritmo de dispersión a versiones concatenadas de los valores de entrada, en lugar de aplicarlo a cada entrada individual por sí sola. Estas medidas reducen considerablemente el riesgo de ataques de reidentificación basados en grandes diccionarios de valores *hash* precomputados.
- El acceso a la base de datos del RMTC está restringido a usuarios con acceso físico al lugar donde se alojan los servidores o con acceso a una conexión VPN establecida para BCB Medical.