

Suscríbete a DeepL Pro para poder editar este documento.  
Entra en [www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document) para más información.

HealthID - Seguridad de la información

Introducción:

Tener información personal en la cadena de bloques no es seguro por varias razones. La blockchain está diseñada para ser inmutable, lo que significa que una vez que los datos se registran en ella, no pueden alterarse ni borrarse. Se trata de una característica fundamental para garantizar la integridad de los registros. Sin embargo, si la información personal se registra de forma irreversible, cualquier error o violación de la privacidad no podrá corregirse.

En lugar de almacenar información personal directamente en la cadena de bloques, es más seguro utilizarla para gestionar los permisos de acceso y controlar el intercambio de datos personales almacenados de forma segura en sistemas externos, siguiendo estrictas normas de privacidad. Esto ayuda a proteger la privacidad de las personas al tiempo que se aprovechan las ventajas de la tecnología.

En nuestro proyecto tratamos la información médica del usuario, por lo que necesitamos tratar esta información y garantizar la privacidad del usuario, y sólo entonces insertar su historial médico en la base de datos.

1. Identificación de datos sensibles:

En la aplicación, el usuario cargará su reconocimiento médico. Una vez cargado, el archivo debe convertirse en texto y se utilizará OCR (reconocimiento óptico de caracteres) para analizar y buscar información sensible (en la cadena de bloques solo deben almacenarse datos no sensibles o información seudonimizada). La información personal que no sea esencial para el propósito de la transacción en la cadena de bloques (liberar el acceso a datos médicos) se eliminará y almacenará de forma centralizada utilizando técnicas de anonimización.

2. Separación física de los datos:

Una forma de separar los datos es crear distintos tipos de registros o estructuras de datos, por ejemplo: **registro de metadatos,** este registro contendrá información de control y metadatos sobre el archivo, como identificadores únicos, fechas de creación, tipos de documentos y cualquier otra información no sensible que sea útil y **registro de contenido,** este registro contendrá el contenido real de los documentos, pero con los datos sensibles anonimizados. Esto significa que la información personal, como nombres y números de identificación, se sustituye por seudónimos.

3. Referencias cruzadas:

Para asegurarse de que el registro de metadatos y el de contenido están relacionados, puede utilizar un identificador único (como un código hash o ID) que vincule estos registros. De este modo, podrás recuperar datos sensibles cuando sea necesario, pero sólo si se concede la autorización correspondiente.

4. Control de acceso:

Implantaremos un sistema de control de acceso mediante contratos inteligentes para garantizar que solo las partes autorizadas puedan acceder a los datos sensibles. Esto te permite definir permisos detallados sobre quién puede ver o utilizar estos datos.

5. Auditoría y trazabilidad:

Registraremos todas las transacciones y actividades relacionadas con el acceso y uso de datos, incluidas las autorizaciones concedidas y revocadas. Esto proporciona trazabilidad y un historial completo de las interacciones con datos sensibles.

6. Cumplimiento de la normativa:

Todas las prácticas de anonimización, seudonimización y almacenamiento de datos deben cumplir la normativa sobre privacidad de datos, como el GDPR de la Unión Europea.

7. Educación de los usuarios:

Hay que informar a los usuarios sobre cómo se protegen sus datos y cómo pueden controlar el acceso a esta información, lo que puede hacerse periódicamente.