EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LA ADOPCIÓN DE TÉCNICAS DE SEUDONIMIZACIÓN

El caso del sector sanitario

MARZO DE 2022

ACERCA DE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, la capacitación y las campañas de sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Para más información sobre la ENISA y su labor, puede consultar: www.enisa.europa.eu.

INFORMACIÓN DE CONTACTO

Para ponerse en contacto con los autores, utilice la dirección de correo isdp@enisa.europa.eu. Las consultas de los medios de comunicación acerca de este documento deben realizarse a través de press@enisa.europa.eu.

CONTRIBUCIONES

Fabio Guasconi (Bl4ckswan), Pantelis Angelidis (UOWM & Vidavo), Prokopios Drogkaris (ENISA)

EDITOR

Prokopios Drogkaris (ENISA)

AGRADECIMIENTOS

Queremos dar las gracias a los miembros del Grupo de Expertos en Seguridad de la Sanidad Electrónica de la ENISA[1] Fotios Gioulekas, Merja Ikäheimonen, Konstantinos Chondropoulos, Ben Kokx, Martha De Cunha Maluf-Burgman, Marta Carbonell Cobo y a los compañeros de la ENISA Athanasios Drougkas y Athena Bourka por sus valiosos comentarios y revisión del documento.

AVISO LEGAL

[1] https://resilience.enisa.europa.eu/ehealth-security

AVISO SOBRE LOS DERECHOS DE AUTOR

ISBN 978-92-9204-576-0, DOI 10.2824/092874

ÍNDICE

RESUMEN EJECUTIVO

A medida que el sector sanitario evoluciona hacia un sector que saca el máximo partido a los avances técnicos y adapta los servicios para satisfacer oportunamente las crecientes necesidades de los pacientes, surgen retos adicionales en materia de ciberseguridad y protección de datos. Integrar nuevas tecnologías en unas infraestructuras informáticas ya complejas de por sí plantea nuevos desafíos en cuanto a la protección de datos y la ciberseguridad.

Esto se debe a la creciente necesidad de intercambiar y compartir información relativa a la salud de los pacientes entre las distintas partes interesadas. Por lo tanto, es importante que, por una parte, las entidades que tratan datos personales recojan y traten posteriormente únicamente los datos que necesitan y, por otra, que adopten medidas organizativas y técnicas adecuadas para proteger dichos datos personales.

La seudonimización se está convirtiendo en una importante técnica de seguridad que proporciona un medio que facilita el tratamiento de datos personales y ofrece, al mismo tiempo, sólidas garantías para proteger los datos personales y, por tanto, salvaguardar los derechos y libertades de las personas.

El presente informe, que complementa los trabajos pertinentes anteriores de la ENISA, demuestra cómo puede adoptarse la seudonimización en la práctica para proteger mejor los datos sanitarios durante el tratamiento. No cabe duda de que no existe una solución única sobre cómo y cuándo aplicar esta técnica; de hecho, se podrían obtener resultados igualmente buenos con otras soluciones en casos específicos, en función de los requisitos de protección, la utilidad, la escalabilidad, etc.

La seudonimización puede ser desde una opción «sencilla» hasta un proceso muy complejo, tanto a nivel técnico como organizativo. Por este motivo, es realmente importante definir tanto las metas y los objetivos de la seudonimización en cada caso particular como la operación de tratamiento.

En el presente informe se destaca el valor añadido que tiene la seudonimización para el sector sanitario y demuestra su aplicabilidad a través de casos de uso sencillos pero concretos. Como complemento de las publicaciones de la ENISA en este ámbito, el presente informe muestra cómo estas técnicas pueden proteger mejor los datos personales tratados en el ámbito de la asistencia sanitaria y, en última instancia, promover dichas medidas técnicas y concienciar sobre su facilidad de uso y su aplicación.

1. INTRODUCCIÓN

En las últimas décadas hemos sido testigos de los veloces avances en el desarrollo y la adopción de nuevas tecnologías. Estos rápidos cambios tecnológicos también han llegado al sector sanitario, que se está digitalizando y adopta continuamente nuevas tecnologías para mejorar la atención a los pacientes, ofrecer nuevos servicios centrados en la atención a domicilio de los pacientes e incluso en planes de prevención.

Integrar nuevas tecnologías en unas infraestructuras informáticas ya complejas de por sí plantea nuevos desafíos en cuanto a la protección de datos y la ciberseguridad, ya que existe una necesidad creciente de intercambiar y compartir información relativa a la salud de las personas entre las distintas partes interesadas, en algunos casos entre países, con el fin de ofrecer mejores servicios sanitarios. Por lo tanto, es importante que las entidades que tratan datos personales recojan y traten posteriormente únicamente los datos que necesiten y, además, adopten medidas organizativas y técnicas adecuadas para proteger dichos datos.

Integrar nuevas tecnologías en el sistema sanitario plantea nuevos desafíos en cuanto a la protección de datos y la ciberseguridad.

La seudonimización es una medida ampliamente conocida que puede contribuir significativamente a este fin.

En términos generales, la seudonimización tiene por objeto proteger los datos personales ocultando la identidad de las personas en un conjunto de datos, por ejemplo, sustituyendo uno o varios identificadores personales[2] por los denominados seudónimos (y protegiendo adecuadamente el vínculo entre los seudónimos y los identificadores iniciales).

No se trata en absoluto de un proceso nuevo en el diseño de los sistemas de información, pero sí ha recibido especial atención tras la adopción del Reglamento general de protección de datos (RGPD) [1], en el que la seudonimización se menciona explícitamente como una técnica que puede promover la protección de datos desde el diseño (artículo 25 del RGPD), así como la seguridad del tratamiento de datos personales (artículo 32 del RGPD).

1.1 LA TRANSFORMACIÓN DIGITAL DEL SECTOR SANITARIO

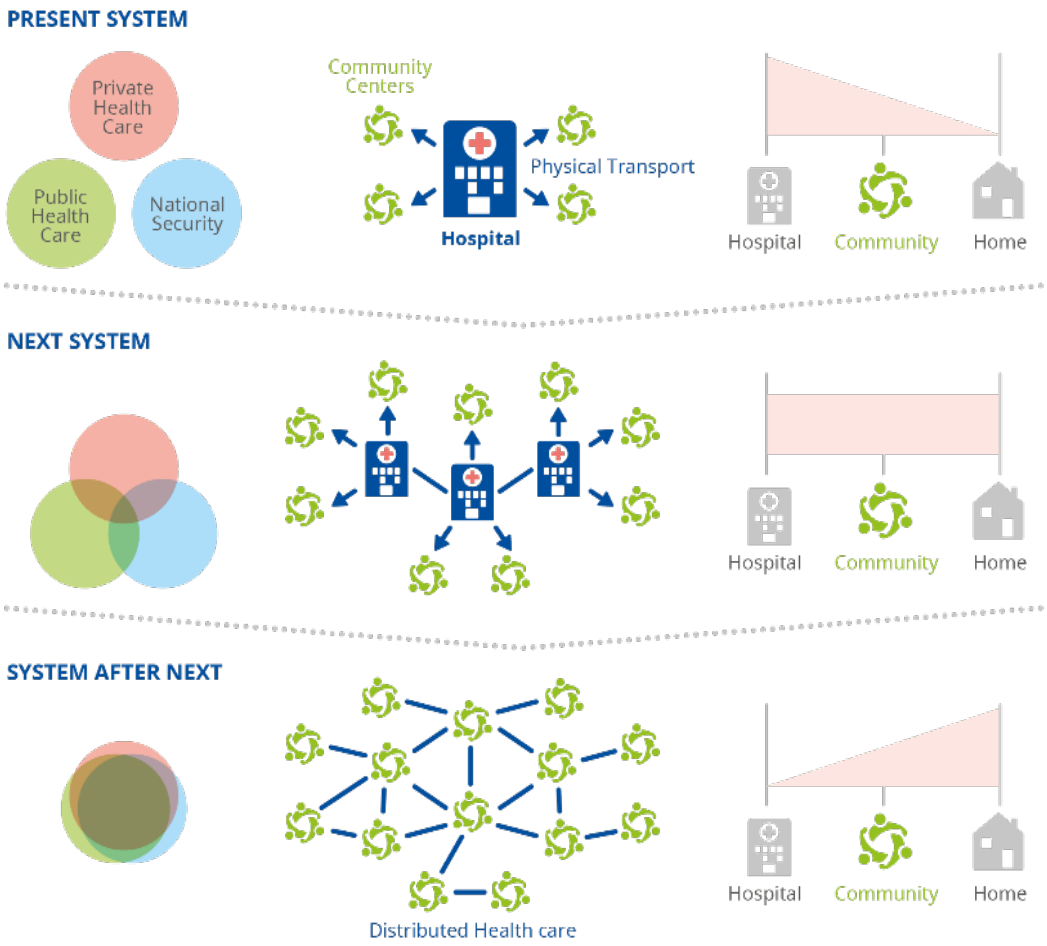
Los datos sanitarios siempre han sido una valiosa fuente de conocimientos en el ámbito de la asistencia sanitaria. Históricamente, este ámbito ha generado enormes cantidades de datos, tanto para el tratamiento de los pacientes como para la investigación y el análisis posterior. Los datos se trataban principalmente en papel, pero en las últimas décadas la accesibilidad y la cantidad de datos digitalizados han aumentado enormemente.

Más recientemente, han surgido numerosas nuevas fuentes de datos sanitarios como resultado del uso generalizado de historiales médicos electrónicos, aplicaciones sanitarias y dispositivos electrónicos ponibles [2]. Además, los avances en la potencia computacional han favorecido el desarrollo de nuevas técnicas de análisis de datos y de aprendizaje automático que ayudan en el diagnóstico, el tratamiento y la administración en la asistencia sanitaria.

Como resultado, se están cambiando los planteamientos y las hospitalizaciones están perdiendo terreno a favor de un sistema de asistencia sanitaria más repartido y que corre a cargo de operadores tanto públicos como privados, todo ello en un entorno más cercano al domicilio del paciente, como se muestra en el gráfico 1.

[2] Un identificador permite la identificación, directa o indirecta, de una persona; por ejemplo, pueden ser identificadores el nombre, la dirección, la fecha de nacimiento, el número de identificación nacional, el número de seguridad social, etc.

Gráfico 1: Desplazamiento del valor en la asistencia sanitaria como consecuencia de la transformación digital [3]



Estos avances tecnológicos han aumentado la demanda de bancos de macrodatos médicos para ofrecer soluciones, por ejemplo, para el diagnóstico y el fenotipado de enfermedades, la modelización de los resultados clínicos, la predicción de estrategias de intervención temprana, la medicina de precisión, etc. Sin embargo, el creciente tratamiento de datos médicos digitalizados también ha incrementado los riesgos en términos de ciberseguridad, protección de datos y probabilidad de violaciones de la seguridad de los datos.

Estos riesgos y las amenazas conexas ya se han identificado en las publicaciones pertinentes de la ENISA en el ámbito de la seguridad de la sanidad electrónica [4], [5] y [6]. Los instrumentos jurídicos pertinentes de la UE, como la Directiva SRI[7], el Reglamento general de protección de datos [1], el Reglamento sobre los productos sanitarios [8], la Directiva relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza[9] etc., impusieron obligaciones a los proveedores de asistencia sanitaria y a los fabricantes de productos sanitarios para garantizar un nivel adecuado y uniforme de protección de los datos médicos y de los productos y servicios que los utilizan.

1.2 PROTECCIÓN DE LOS DATOS SANITARIOS

La protección de los datos sanitarios se considera una cuestión de alta prioridad debido a su carácter sensible y a la importancia que tienen para las personas («los interesados»). Desde el

punto de vista de la ciberseguridad, confidencialidad, disponibilidad e integridad de los datos médicos y de la infraestructura pertinente se consideran esenciales para poder prestar una atención médica oportuna, adecuada e ininterrumpida.

Esto también se pone de relieve en la Directiva SRI[7], que clasifica al sector sanitario como operador de servicios esenciales y pide unos requisitos mínimos de seguridad para garantizar un nivel de seguridad adecuado al nivel de los riesgos presentados. Además, el RGPD distingue, en su artículo 9, los datos relativos a la salud como una categoría especial de datos (sensibles) y establece requisitos adicionales y obligaciones más estrictas para el tratamiento y la protección de dichos datos, con el fin de salvaguardar los derechos y libertades de las personas («los interesados»). Por último, el Reglamento sobre los productos sanitarios impone requisitos relativos a la seguridad, la calidad y la protección de los productos sanitarios con el fin de alcanzar un elevado nivel común de seguridad.

1.3 ÁMBITO DE APLICACIÓN — PÚBLICO DESTINATARIO

El objetivo del presente informe es destacar el valor añadido de la seudonimización en el sector sanitario y demostrar su aplicabilidad a través de casos de uso sencillos pero específicos. Como complemento de las publicaciones pertinentes de la ENISA en este ámbito [10], [11], [12], el objeto del presente informe es mostrar cómo estas técnicas pueden proteger mejor los datos personales tratados en el ámbito de la asistencia sanitaria y, en última instancia, promover dichas medidas técnicas y concienciar sobre su facilidad de uso y su aplicación.

Este documento está destinado a los profesionales y desarrolladores de tecnologías de la información en el ámbito de la asistencia sanitaria, así como a las autoridades sanitarias, que pueden presentar recomendaciones sobre la seguridad del tratamiento de datos sanitarios.

1.4 ESTRUCTURA DEL DOCUMENTO

En el apartado 2 se presenta la seudonimización y se analizan sus ventajas y las técnicas más comunes que se utilizan. En el apartado 3 se muestra el uso de la seudonimización en tres casos de uso que se centran en la recogida de datos sanitarios de pacientes y el tratamiento de dichos datos por parte de los proveedores de asistencia sanitaria y los centros de investigación médica. Por último, en el apartado 4 se exponen las principales conclusiones y recomendaciones pertinentes.

2. SEUDONIMIZACIÓN

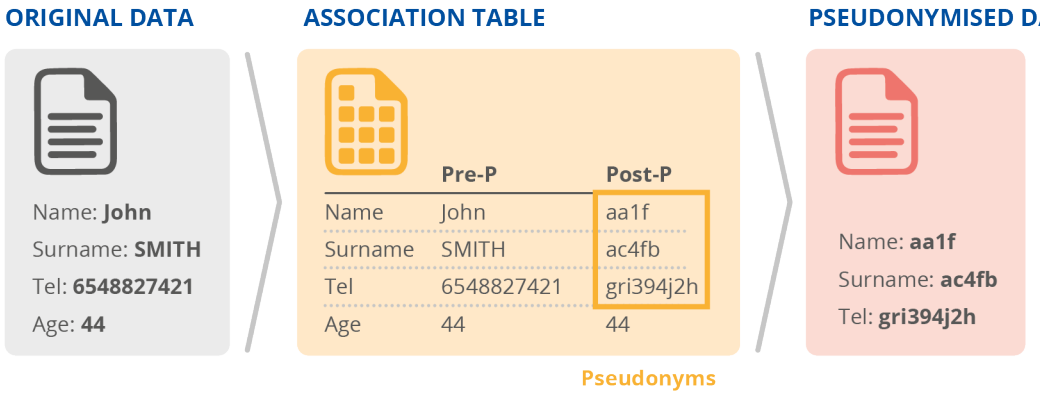
2.1 CONTEXTO

El RGPD define la seudonimización en el artículo 4, apartado 5, como: «*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*».

En términos generales, la seudonimización tiene por objeto proteger los datos personales ocultando la identidad de las personas (los interesados) en un conjunto de datos, por ejemplo, sustituyendo uno o varios identificadores de datos personales por los denominados seudónimos y protegiendo adecuadamente el vínculo entre los seudónimos y los identificadores iniciales. Este vínculo, conocido a menudo como secreto de seudonimización, suele almacenarse en una tabla de correspondencia y puede utilizarse para volver a identificar a la persona asociando los seudónimos a los datos originales, tal como se muestra en el gráfico 2. Únicamente puede acceder a la tabla de correspondencia la entidad que realizó inicialmente la seudonimización, a la que se suele denominar «entidad de seudonimización».

La seudonimización es una técnica bien establecida que tiene por objeto proteger los datos personales ocultando la identidad de las personas.

Gráfico 2: Ejemplo de seudonimización



La seudonimización es una de las distintas técnicas de «desidentificación» (como la agregación, la ofuscación, el enmascaramiento, etc.) destinadas a eliminar la asociación entre un conjunto de datos de identificación y el sujeto de los datos. Otras definiciones de seudonimización, como las de la ISO y, en concreto, la ISO 25237: 2017, «Informática sanitaria — seudonimización» [13], se basan en esta principio y son similares a la definición del RGPD antes mencionada.

2.2 LA IMPORTANCIA DE LA SEUDONIMIZACIÓN

La principal ventaja de la seudonimización, cuando se aplica correctamente, es que permite ocultar la identidad de una persona en el contexto de un conjunto de datos específico, de modo que no sea posible asociar los datos a la persona en cuestión. Por lo tanto, también ayuda a reducir el riesgo de vincular datos personales de una persona concreta en diferentes ámbitos de tratamiento de datos.

De este modo, por ejemplo, si se produce una violación de la seguridad de los datos personales, la seudonimización dificulta a quienes no sean el responsable del tratamiento la

tarea de asociar los datos vulnerados a determinadas personas sin usar información adicional. Es importante indicar que además puede reducir el nivel de riesgo al que están expuestos los datos seudonimizados.

La diferencia radica en saber que nuestro ejemplo «John SMITH» del gráfico 2 padece una enfermedad crónica y que una persona identificada como «aa1f ac4fb» padece una enfermedad crónica. Incluso aunque se filtraran datos seudonimizados, una tercera empresa no podrá dirigir a John SMITH sus campañas de *marketing* basadas en esa información, a menos que la información sobre el mecanismo de asociación de seudónimos a los interesados también se vea comprometida.

El uso de datos seudonimizados debería, por ejemplo, dar más confianza a los interesados a la hora de dar su consentimiento al uso de sus datos sanitarios con fines de investigación e incluso aumentar la eficacia de otros controles de seguridad que deben aplicarse a datos no seudonimizados, como, por ejemplo, el cifrado.

Por último, cabe señalar que la seudonimización y la anonimización no siguen el mismo proceso y que el RGPD considera que los datos seudonimizados son datos personales, mientras que los datos anónimos no lo son[3].

2.3 TÉCNICAS BÁSICAS DE SEUDONIMIZACIÓN

Tal y como se explica en [10], [11] y [12], existen varias técnicas de seudonimización. Las principales diferencias entre ellas radican en cómo se genera el seudónimo. En el cuadro 1 que figura a continuación se ofrece un resumen exhaustivo de las más comunes.

Cuadro 1: Resumen de las técnicas básicas de seudonimización

Técnica	Generador de seudónimos
Contador	Contador de función monótona que comienza con un determinado valor que se va incrementando cuando se necesita un nuevo seudónimo
Número aleatorio	Valor aleatorio extraído entre un límite mínimo y un límite máximo cuando se necesita un nuevo seudónimo
Función resumen (*hash*)	Función criptográfica de un solo sentido (no reversible) que transforma los datos personales de entrada en valores de longitud fija
Código de autentificación de mensaje resumido (HMAC)	Función criptográfica de un solo sentido (no reversible) que añade una clave que la hace menos predecible que una función resumen (*hash*)
Cifrado	Función criptográfica bidireccional (reversible) que transforma los datos personales de entrada en valores que pueden volver a transformarse en su formato original utilizando una clave

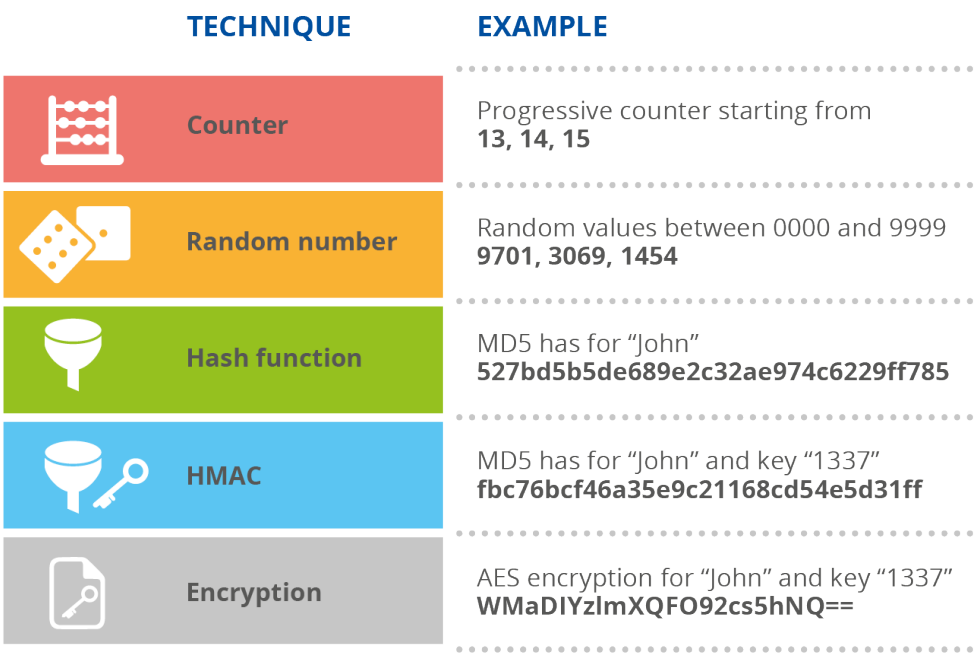
Tal como se menciona en [10], aunque la función de resumen (*hash*) puede contribuir de manera significativa a garantizar la integridad de los datos, normalmente se considera una técnica de seudonimización débil, puesto que es vulnerable a los ataques de fuerza bruta y de

[3] Puede ampliarse la información sobre las técnicas de anonimización en el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo 29.

diccionario. Del mismo modo, los contadores también se consideran una técnica de seudonimización débil, ya que no pueden escalarse.

Un enfoque sólido para generar seudónimos puede consistir en utilizar funciones *hash* con clave como se muestra en el gráfico 8, es decir, funciones *hash* cuyo valor de salida no depende solo del valor de entrada, sino también de una clave secreta (sal). En el gráfico 3 se presentan algunos ejemplos prácticos de la aplicación de las técnicas mencionadas:

Gráfico 3: Aplicación de técnicas básicas de seudonimización

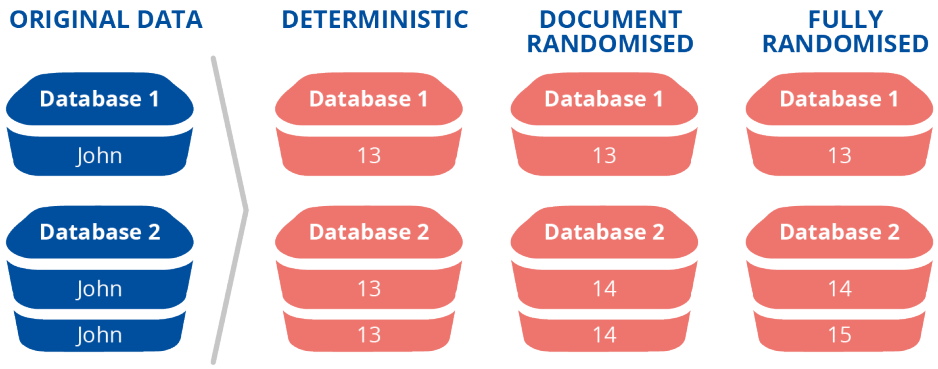


La diferencia entre las tres últimas técnicas ilustradas en el cuadro 1 y en el gráfico 3 puede que no se aprecie inmediatamente; no obstante, es sustancial en cuanto a la aplicación de dichas técnicas, al igual que también clave elegir el alcance y el enfoque, es decir, la política con la que se aplicarán dichas técnicas. En general, la política podría implicar:

1) la **seudonimización determinista**: utilizar siempre el mismo seudónimo para los mismos datos;
2) la **seudonimización aleatoria de documento**: utilizar seudónimos iguales para los mismos datos únicamente dentro de un mismo ámbito de aplicación;
3) la **seudonimización totalmente aleatorizada**: utilizar siempre un seudónimo diferente para los mismos datos.

En el gráfico 4 se muestran las políticas aplicadas a la técnica del contador, comentada anteriormente, en tres casos con los mismos datos personales en dos bases de datos diferentes:

Gráfico 4: Aplicación de las políticas de seudonimización



En la práctica, existen métodos más avanzados y, dado que se trata de un tema de gran interés, las técnicas también están evolucionando pero, en general, se tiende a combinar las técnicas más comunes descritas anteriormente o a introducir una serie de variaciones.

2.4 CONSIDERACIONES SOBRE LA SEUDONIMIZACIÓN

Los responsables y los encargados del tratamiento de datos pueden utilizar técnicas de seudonimización y políticas conexas ya sea de forma conjunta —utilizando los mismos criterios— o por separado. El primer caso suele darse cuando el responsable del tratamiento necesita que el encargado del tratamiento adopte los mismos criterios. Aparte del uso de criterios, la diferencia más importante sería la puesta en común de la tabla de correspondencia que figura en el gráfico 2.

Si no se comparte esta tabla, la entidad que recibe datos seudonimizados —siempre que todos los mecanismos se apliquen correctamente— no tendría forma de recuperar los datos personales originales. Si se comparte la tabla, deberá hacerse con la misma atención que se presta al intercambio de claves de cifrado, salvo por las posibles diferencias debidas al mayor volumen de datos.

Un responsable del tratamiento de datos puede pedir a los encargados que seudonimicen los datos personales o incluso indicarles cómo hacerlo, especialmente si los datos seudonimizados deben intercambiarse entre distintas partes. Dichas especificaciones deben incluir al menos los siguientes elementos y basarse siempre en los resultados de evaluaciones de riesgo o impacto realizadas previamente:

- los **datos personales** objetivo (por ejemplo, un conjunto de identificadores);
- la **técnica** que va a utilizarse;
- los **parámetros** aplicables a la técnica (por ejemplo, la lógica del contador, la gestión de la aleatoriedad, los algoritmos empleados, las longitudes de clave);
- la **política** que va a utilizarse.

En función de los requisitos aplicables, que probablemente incluirán la normativa, la velocidad, la simplicidad, la previsibilidad y el presupuesto, la técnica y los parámetros conexos podrían variar.

3. CASOS DE USO

En un intento de demostrar el valor añadido de la seudonimización en el ámbito de la asistencia sanitaria, en este apartado se presentan tres casos de uso en los que se han seudonimizado los datos médicos personales sujetos al tratamiento. Aunque no se analizan en profundidad técnicas específicas de seudonimización, con los diferentes casos de uso se intenta ofrecer una visión general de las posibilidades y los aspectos clave de su aplicación, en cuanto al mayor nivel de protección de los datos personales tratados gracias a la supresión de identificadores personales directos.

Cabe señalar que estos casos de uso sirven para demostrar la aplicación de la seudonimización y no pretenden abarcar los casos de uso operativo en toda su extensión. En tales supuestos, habría que analizar más en profundidad el contexto, los encargados del tratamiento y el tratamiento de datos implicado, así como todas las operaciones de tratamiento pertinentes.

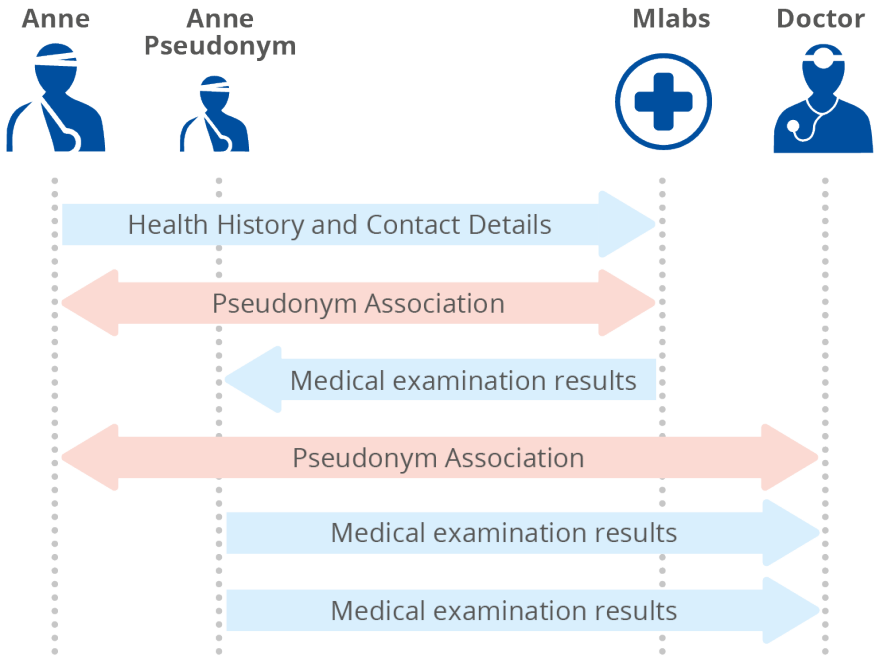
3.1 EL INTERCAMBIO DE DATOS SANITARIOS DE PACIENTES

En la práctica médica actual, el intercambio de datos entre organizaciones es una práctica común y se utiliza principalmente con fines diagnósticos y terapéuticos. Aquí se incluyen los intercambios entre diferentes unidades de la misma entidad (por ejemplo, un hospital) y el intercambio entre destinatarios concretos (por ejemplo, profesionales médicos, laboratorios, etc.).

Por ejemplo, Anne realiza una serie de pruebas médicas en el laboratorio médico Mlabs que posteriormente deben ser estudiadas por su médico. Cuando Anne visita Mlabs por primera vez, se le pide que facilite información sanitaria contextual (medicación, historial médico, etc.) y datos personales (nombre, datos de contacto, número de seguridad social) y Mlabs le asigna un ID_Paciente. A partir de este momento, todos los datos, como los resultados, etc. relacionados con un control médico se asocian a este ID_Paciente y no a sus datos personales, como se muestra en el gráfico 6. El identificador del paciente, que puede incluso ser un simple contador de registro progresivo, se utiliza para disociar los datos personales de Anne de los resultados y actúa como un seudónimo simple pero eficaz.

Los datos que se transfieren de Mlabs al médico tratante no contienen los identificadores personales de Anne, sino únicamente el seudónimo y los resultados de las pruebas médicas.

Gráfico 5: El intercambio de datos sanitarios de pacientes

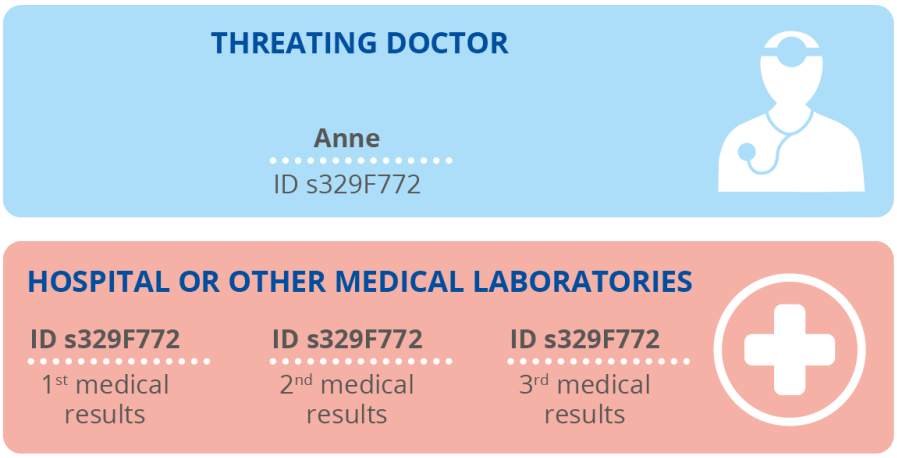


Una vez finalizadas las pruebas médicas, Mlabs asociará los resultados del laboratorio al ID_Paciente y no a los datos personales. Cuando Anne solicite una copia de los resultados, Mlabs tendrá que buscar el ID_Paciente que le ha asignado y, a continuación, realizar la correspondencia, ya que el ID_Paciente y los datos personales se almacenan por separado.

Si la paciente solicita que se manden los resultados directamente a su médico tratante, que será el responsable de analizarlos y decidir si se necesitan más pruebas o medicación, Mlabs puede informar al médico de los resultados del ID_Paciente asignado a Anne. La asociación entre Anne e ID_Paciente debe comunicarse al médico tratante una sola vez; posteriormente, el médico ya sabrá que ese ID_Paciente concreto se refiere a Anne. Sin embargo, en este punto, el médico obtiene acceso al secreto de seudonimización y puede identificar directamente a Anne, lo que pone fin al nivel de protección de los datos personales que ofrece el proceso de seudonimización realizado anteriormente. Este nivel de protección seguiría vigente si Anne solo compartiera los resultados de las pruebas médicas y no el secreto de seudonimización.

El mismo principio puede extenderse a una entidad, como un hospital, donde un paciente se somete a diferentes pruebas en varias unidades clínicas. Una vez más, las unidades que realizan las pruebas procesarán los datos utilizando el ID_Paciente y el médico tratante podrá relacionar dicho identificador con Anne como se muestra a continuación. El acceso a datos médicos entre los facultativos del mismo centro médico (por ejemplo, un hospital) debe basarse en la autenticación y en los derechos de usuario pertinentes. En función de la operación de tratamiento, los médicos podrían tener acceso al secreto de seudonimización, con lo que podrían identificar directamente a Anne, o tener acceso únicamente al identificador seudonimizado de Anne, por lo que no podrían identificarla directamente.

Gráfico 6: La disociación de seudónimos



Cabe señalar que este caso de uso no se aplica directamente a aquellos casos en que ya se utilizan sistemas de historiales médicos electrónicos o historiales médicos electrónicos interoperables[4], puesto que aquí ya podían definirse los medios para la comunicación de datos y la identificación de personas. Sin embargo, en tales casos, la seudonimización podría utilizarse en las primeras fases de diseño como técnica para aumentar el nivel de protección, apoyar el cumplimiento normativo y promover una adopción más amplia de los historiales médicos electrónicos.

Los datos seudonimizados de los ensayos clínicos permiten detectar asociaciones durante los ensayos y volver a identificar a personas concretas si fuera necesario.

3.2 ENSAYOS CLÍNICOS

Los ensayos clínicos estudian nuevos procedimientos y tratamientos médicos y evalúan sus efectos y posibles efectos adversos. Se consideran un requisito previo para obtener las autorizaciones necesarias de las autoridades competentes. Por lo general, no los realiza el fabricante (por ejemplo, la empresa farmacéutica), sino organizaciones independientes denominadas «organizaciones de investigación clínica».

Un caso típico es el denominado estudio doble ciego, en el que una cohorte de individuos con características similares (por ejemplo, pacientes con la misma enfermedad) se divide en dos subgrupos. Los miembros de un grupo reciben la medicación objeto del ensayo y los miembros del otro grupo, un placebo. En un estudio doble ciego, ni los participantes ni el investigador saben quién pertenece a cada grupo. Durante el ensayo, se recogen los mismos datos médicos para ambas cohortes. Una vez obtenidos todos los datos, los investigadores pueden comparar los resultados de cada grupo y determinar si la nueva mediación médica (variable independiente) ha tenido algún impacto en el tratamiento (variable dependiente).

Más allá de la mera comparación de los registros de datos de los pacientes, otro uso común de estos datos médicos es la detección de asociaciones y patrones entre diferentes variables (por ejemplo, edad, sexo, ocupación), con miras a identificar el límite superior de eficiencia y eficacia, así como información de seguridad adicional, por ejemplo, sobre la posología. Por lo tanto, en estas organizaciones de investigación, deben analizarse los datos de todos los pacientes para establecer patrones comunes con relevancia médica.

Para estos análisis, la identidad de los participantes no tiene una importancia directa, y normalmente los investigadores no necesitan acceder a la identidad real de los participantes en la investigación cuyos datos analiza la organización de investigación clínica. Sin embargo, el

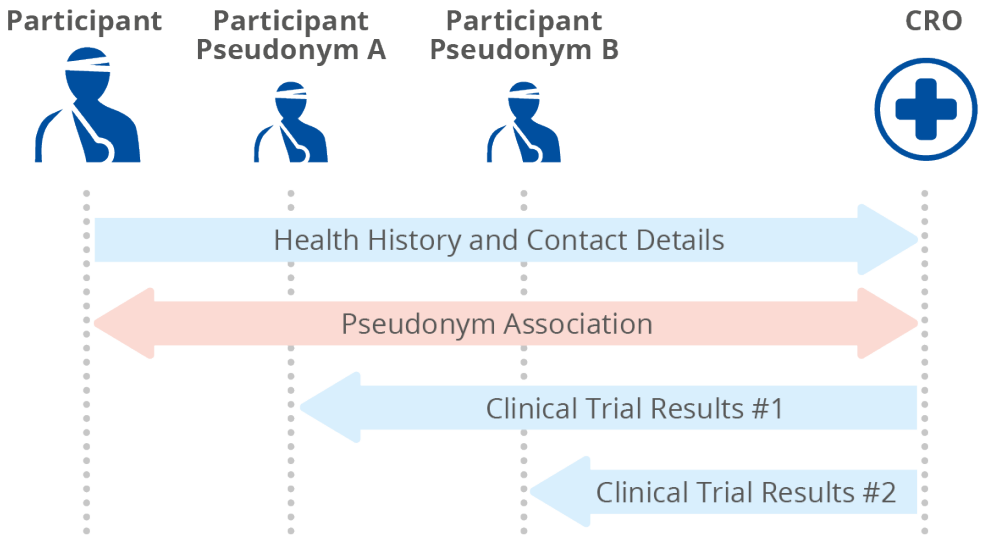
[4] Recomendación de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo, C (2019) 800 final.

riesgo de que un paciente sea identificado a través de información indirecta no es mínimo. En el caso de los ensayos clínicos, información como la edad, el sexo, la ocupación o el lugar de residencia puede ser pertinente para el estudio y, en determinadas condiciones, puede llevar a la identificación de los participantes en el ensayo.

En este contexto, un sistema de seudonimización adecuado resultaría óptimo para llevar a cabo las tareas de detección de asociaciones y patrones estadísticos sin revelar el valor real de las diferentes entradas de datos. En algunos ensayos, esto puede extenderse incluso a las asociaciones y los patrones estadísticos de los síntomas y la medicación. Dado que, durante los ensayos clínicos, suelen recogerse varios tipos de datos personales, la seudonimización debe hacerse con atención para no exponer a los pacientes a una reidentificación no autorizada. Para ello podrían combinarse dos enfoques, por ejemplo, como se muestra en el gráfico 8:

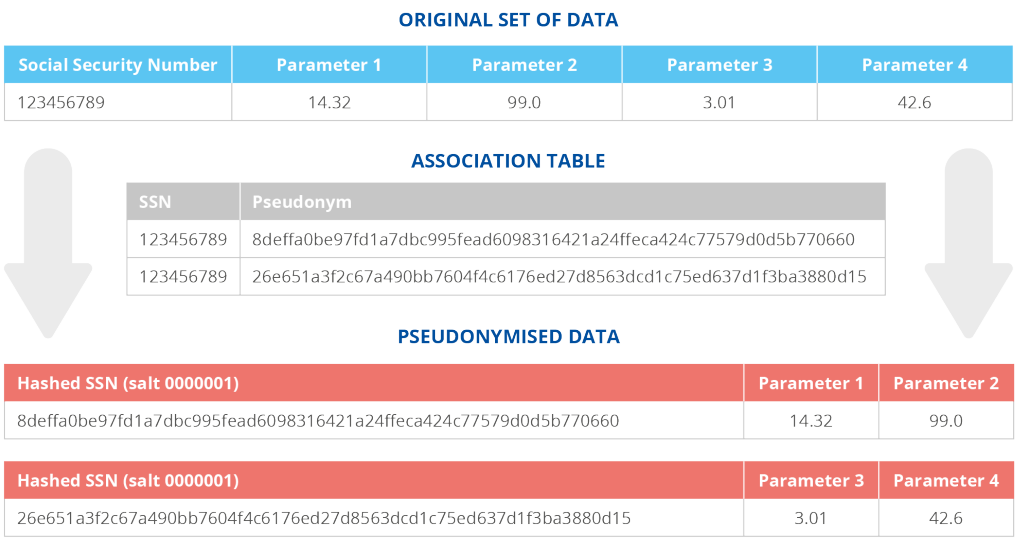
1) emplear la seudonimización en los principales datos de identificación de cada participante;
2) utilizar más de un seudónimo para cada dato de identificación de diferentes parámetros clínicos.

Gráfico 7: Resumen de la seudonimización en los ensayos clínicos



Este enfoque podría limitar los datos personales relacionados con cada seudónimo que, junto con la solidez que puede obtenerse utilizando una función *hash* sólida como SHA-2 con un valor de semilla aleatoria, como se muestra en el ejemplo siguiente, dificultaría aún más la reidentificación.

Gráfico 8: La asociación de los parámetros a los seudónimos



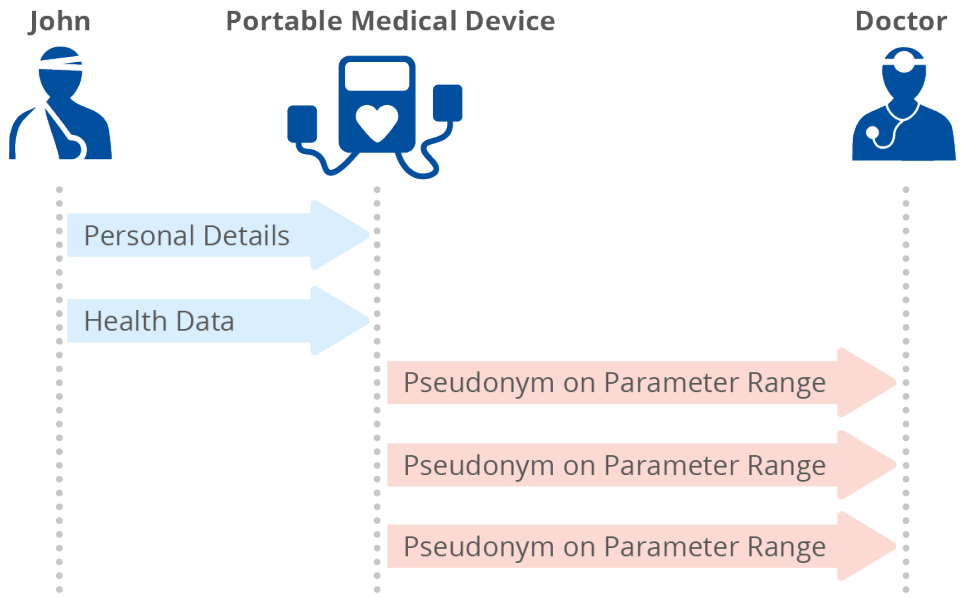
Se puede dar otra excepción a la hipótesis básica cuando los datos de un paciente pueden revelar un riesgo para su salud (por ejemplo, un nuevo diagnóstico) y al equipo de investigación le convendría ponerse en contacto con la organización de investigación clínica y activar una notificación al paciente. Este es un caso muy similar al que se analiza en [12] en el apartado 4.2.2.

3.3 EL SEGUIMIENTO DE LOS DATOS SANITARIOS GENERADOS POR EL PACIENTE

En la actualidad, los dispositivos ponibles inteligentes controlan las constantes vitales como la frecuencia cardíaca, la saturación de oxígeno y la presión arterial. La supervisión periódica de las constantes vitales es una práctica frecuente en la asistencia a los pacientes y ayuda a reconocer de manera temprana parámetros fisiológicos anómalos. Sin embargo, lo habitual es que solo el propio paciente vea las mediciones y se ponga en contacto con el médico cuando observe un valor anómalo.

Los intervalos normales en las constantes vitales de una persona suelen variar en función de la edad, el peso, el sexo y el estado de salud general, lo que dificulta la fijación de valores predefinidos. Este caso de uso contempla la puesta a disposición de un sistema de vigilancia de la salud (HMS) en el que el médico pueda acceder a la información médica y supervisar los signos vitales y recibir también la notificación de sus valores anómalos, a través de rangos de valores adecuadamente predefinidos.

Gráfico 9: La seudonimización en el seguimiento de los datos sanitarios generados por el paciente



La transferencia seudonimizada desde el producto sanitario al médico tratante reduce el riesgo de que los datos se vean comprometidos durante el tránsito.

Por ejemplo, a John se le ha diagnosticado una enfermedad cardiovascular y arritmia; la bradicardia o taquicardia puede aumentar el riesgo de ictus. El médico de John ha definido tres conjuntos de valores en relación con su corazón en reposo: bajo, normal y alto. El dispositivo ponible de John supervisa regularmente su frecuencia cardíaca y actividad física, y le avisa cuando la frecuencia cardíaca en reposo supera los umbrales bajos o altos. Al mismo tiempo, esta notificación también puede enviarse al médico tratante, quien podrá ayudar a John inmediatamente o ponerse más tarde en contacto con él para indicarle qué hacer a continuación.

En vez de transmitir los valores y datos del corazón de John, el dispositivo ponible puede realizar el proceso de seudonimización y transmitir un seudónimo de John y la gama de parámetros de su frecuencia cardíaca en reposo. El médico recibirá el seudónimo y podrá acceder a la información del paciente correspondiente y el estado de la frecuencia cardíaca del paciente en reposo. Al igual que en el caso de uso analizado en el apartado 3.1, si el médico tiene acceso al secreto de seudonimización y puede identificar directamente a John, el proceso de seudonimización se considerará principalmente una medida de seguridad a favor de la confidencialidad durante la transmisión, y no una medida de protección de datos.

Gráfico 10: Tabla de correspondencia de los seudónimos

Si profundizamos más en este caso de uso, el dispositivo ponible podría perfectamente estar sujeto a las disposiciones del Reglamento sobre productos sanitarios [8] y a las orientaciones sobre la ciberseguridad de los productos sanitarios [14] aprobadas por el Grupo de Coordinación de Productos Sanitarios (MDCG). De ser así, la adopción de técnicas de seudonimización, por ejemplo, durante la comunicación y el almacenamiento de datos médicos personales podría ayudar a respetar los principios tanto de seguridad como de protección de datos desde el diseño, y al mismo tiempo reforzar la confidencialidad de los datos transferidos.

4. CONCLUSIONES

A medida que el sector sanitario evoluciona hacia un sector que saca el máximo partido a los avances técnicos y adapta los servicios para satisfacer oportunamente las crecientes necesidades de pacientes de todas las edades y culturas a nivel mundial, surgen retos adicionales en materia de ciberseguridad y protección de datos.

La seudonimización se está convirtiendo en una importante técnica de seguridad que proporciona un medio que facilita el tratamiento de datos personales y ofrece, al mismo tiempo, sólidas garantías para proteger los datos personales y, por tanto, salvaguardar los derechos y libertades de las personas.

El presente informe, que complementa los trabajos pertinentes anteriores de la ENISA, demuestra cómo puede adoptarse la seudonimización en la práctica para proteger mejor el intercambio de datos sanitarios.

No cabe duda de que no existe una solución única sobre cómo y cuándo aplicar la seudonimización; de hecho, se podrían obtener resultados igualmente buenos con otras soluciones en casos específicos, en función de los requisitos de protección, utilidad, escalabilidad, etc.

Partiendo de un simple *token*, la seudonimización puede ser desde una opción «sencilla» hasta un proceso muy complejo, tanto a nivel técnico como organizativo. Por este motivo, es realmente importante definir las metas y los objetivos de la seudonimización en cada caso particular y cada operación de tratamiento. A tal fin, unas buenas prácticas y ejemplos de seudonimización pertinentes en el contexto del RGPD pueden resultar muy valiosos para los proveedores de asistencia sanitaria y los desarrolladores de aplicaciones sanitarias.

Los desarrolladores y reguladores nacionales y europeos deben promover el intercambio de buenas prácticas y ofrecer orientaciones prácticas sobre el uso de la seudonimización.

Los avances en la tecnología y en los tipos de servicios sanitarios que se ofrecen a la población podrían comprometer la eficacia y aplicabilidad de las soluciones de seudonimización actuales. Esto no solo es pertinente para la elección de la técnica, sino también para el diseño general del proceso de seudonimización, que incluye, en particular, la protección de la información adicional (es decir, la información que permite asociar los seudónimos a los identificadores iniciales).

Las soluciones de seudonimización propuestas dependen en gran medida de los avances tecnológicos y, con el paso del tiempo, pueden surgir problemas o limitaciones de aplicación para cada técnica.

La comunidad investigadora debe seguir trabajando en la protección de datos y la ingeniería de seguridad, incluidas las técnicas de seudonimización más avanzadas y sus posibles aplicaciones, con el apoyo de las instituciones de la UE en términos de orientación política y financiación en investigación.

5. BIBLIOGRAFÍA

x

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. (2016)

2. Topol, E.: Individualized Medicine from Prewomb to Tomb. (2014)

3. Angelidis, P.: UOWM Lecture Notes. (2019)

4. ENISA: Security and Resilience in eHealth Infrastructures and Services. (2015)

5. ENISA: Procurement Guidelines for Cybersecurity in Hospitals. (2020)

6. ENISA: Cloud Security for Healthcare Services. (2021)

7. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016)

8. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EE. (2017)

9. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. (2011)

10. ENISA: Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation. (2019)

11. ENISA: Pseudonymisation techniques and best practices. (2019)

12. ENISA: Data Pseudonymisation: Advanced Techniques and Use Cases. (2021)

13. ISO: 25237:2017 Health informatics — Pseudonymization. (2017)

14. Medical Device Coordination Group: 2019-16 - Guidance on Cybersecurity for medical devices. (2019)

x

TP-01-22-221-EN-N

ACERCA DE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, la creación de capacidades y la sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Para obtener más información sobre la ENISA y su trabajo, puede consultar: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-576-0
DOI 10.2824/092874