BLOCKCHAIN™ IN HEALTHCARE TODAY

DE COMPARTIR A VENDER: RETOS Y OPORTUNIDADES DE ESTABLECER UN MERCADO DIGITAL DE DATOS SANITARIOS MEDIANTE TECNOLOGÍAS BLOCKCHAIN

Mohamed A. Maher, MBA[1,2]* e Imtiaz A. Khan, PhD[(1)]

[1]Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, Reino Unido; [2]Balsamee LTD, Cardiff, Reino Unido

Resumen

Durante la pandemia de COVID-19, fuimos testigos de cómo el intercambio de datos biológicos y biomédicos facilitó a investigadores, médicos y responsables políticos hacer frente a la pandemia a escala mundial. A pesar del creciente uso de las historias clínicas electrónicas (HCE) por parte de los médicos y de los dispositivos digitales portátiles por parte de los particulares, el 80% de los datos médicos y sanitarios siguen sin utilizarse, lo que añade poco valor al trabajo de investigadores y médicos. Se cree que las limitaciones legislativas relacionadas con el intercambio de datos sanitarios, el diseño centralizado y aislado de los sistemas tradicionales de gestión de datos y, sobre todo, la falta de modelos de incentivación son los principales obstáculos para el intercambio de datos sanitarios.

Con la llegada del Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) y el desarrollo de tecnologías como blockchain y las tecnologías de libro mayor distribuido (DLT), ahora es posible crear un nuevo paradigma de intercambio de datos cambiando el modelo de incentivación de la forma autoritaria o altruista actual a un modelo económico compartido en el que la incentivación financiera será el principal motor del intercambio de datos. Esto puede lograrse creando un mercado digital de datos sanitarios (DHDM).

Aquí, revisamos artículos que proponen modelos técnicos o marcos implementados que utilizan tecnologías similares a blockchain para datos de salud. Tratamos de comprender y comparar los diferentes retos técnicos asociados a la implementación y optimización del funcionamiento del DHDM esbozado en estos artículos. También examinamos las limitaciones legales en el contexto de la UE y otros países como EE.UU. para dar cabida a cualquier requisito de cumplimiento para un mercado de este tipo. Por último, pero no menos importante, revisamos los artículos que investigaron el impacto socioeconómico a corto, medio y largo plazo de un mercado de este tipo en una amplia gama de partes interesadas.

Palabras clave: *blockchain*; *HCE*; *mercado; GDPR*; *reglamento general de protección de datos*; *incentivos*

Sección: Narrativa/Revisiones sistemáticas/Metaanálisis

Recibido: 22 de septiembre de 2021; Revisado: 27 de septiembre de 2021; Aceptado: 30 diciembre 2021; Publicado: 28 enero 2022

Sesde los inicios de la sanidad digital, los desarrolladores de tecnologías de la información y la comunicación (TIC) han tenido la impresión de que el uso de la tecnología digital en el tratamiento y procesamiento de la información sanitaria generará una gran cantidad de datos que pueden transformar la industria sanitaria. Alimentar estos datos con algoritmos de aprendizaje automático nos permitirá desespecializar la práctica médica y proponer nuevos diagnósticos y procesos de tratamiento. Proyectos como DeepMind Health son un ejemplo reciente: una empresa de inteligencia artificial con sede en Londres y propiedad de Alphabet ha desarrollado una aplicación móvil (1) que utiliza los datos de la HCE del hospital Royal Free de Londres para predecir e identificar a los pacientes que están a punto de morir. del hospital Royal Free de Londres para predecir e identificar a los pacientes que están a punto de sufrir una lesión renal aguda, una afección relacionada con 100.000 muertes al año en el Reino Unido (2). Además, portales como Patients-LikeMe (3), a través del cual pacientes con afecciones o preocupaciones médicas similares pueden compartir información sobre sus tratamientos, tienen beneficios demostrables para sus usuarios (4, 5).

Cuando estos proyectos empezaron a mostrar el valor de compartir datos, el Reglamento General de Protección de Datos (RGPD) (6) de la Unión Europea (UE), introducido en 2018, ha cambiado fun-damentalmente el paradigma de compartir y usar datos de pacientes al reposicionar la propiedad y la administración

*Correspondencia: Mohamed A. Maher. Email:m.maher2@outlook.cardiffmet.ac.uk ; mohamed.maher@balsamee.co.uk

Tabla 1. El Reglamento general de protección de datos de la UE cambió fundamentalmente el paradigma de compartir y utilizar los datos de los pacientes al reposicionar la propiedad y la administración de los datos médicos de los proveedores de servicios al paciente, junto con la concesión de los siguientes derechos (6)

Reglamento general de protección de datos	Definido en
Artículos 12 y 13 del RGPD	Derecho a ser informado • Derecho de las personas a ser informadas sobre la recogida y el uso de sus datos.
Artículo 15 del RGPD	Derecho de acceso: • Las personas tienen derecho a acceder a sus datos.
Artículo 16 del RGPD	Derecho de rectificación: • Derecho de los individuos a que se modifiquen o completen los datos personales no correctos si estaban incompletos.
Artículo 17 del RGPD	Derecho de supresión: • El derecho de los individuos a que se borren los datos personales, es decir, normalmente llamado "el derecho a ser olvidado."
RGPD, artículo 18	Derecho a restringir el tratamiento: • Derecho de las personas a solicitar la restricción o supresión de sus datos.
Artículo 20 del RGPD	Derecho a la portabilidad de los datos • Permite a las personas transportar, trasladar, copiar o enviar sus datos fácilmente de un sistema informático a otro de forma segura, sin que ello afecte a su usabilidad.
Artículo 21 del RGPD	Derecho de oposición • Las personas tienen derecho a oponerse al tratamiento de sus datos en determinadas circunstancias.
Artículo 22 del RGPD	Derechos relativos a la toma de decisiones automatizada y la elaboración de perfiles: • Normas para proteger a las personas, si una organización está llevando a cabo una toma de decisiones automatizada que tiene efectos significativos sobre ellas.

de datos médicos del proveedor de servicios al paciente, junto con el otorgamiento de los siguientes derechos enumerados en el cuadro 1.

Si DeepMind no hubiera iniciado antes de la introducción del GDPR o PatientsLikeMe estuviera dentro de la jurisdicción del Espacio Económico Europeo (EEE), ninguno de los proyectos mencionados podría siquiera iniciarse. Ahora es más evidente que los datos tienen un único propietario y guardián en lo que respecta a los derechos de acceso o distribución. Incluso de forma anónima, sólo el paciente tiene derecho a conceder acceso a sus datos y permitir que se utilice la información de forma que beneficie a todos. Irónicamente, los pacientes aún no han reconocido el valor de este nuevo derecho de propiedad ni cómo gestionar su administración. Esto se debe a que no se han creado ganancias directas que les sirvan, así como ganancias indirectas, que no son lo suficientemente claras como para superar las preocupaciones legítimas de la fuga de datos y la consiguiente exposición de la privacidad. Por lo tanto, el objetivo es encontrar un nuevo enfoque y herramientas que equilibren la privacidad individual y el acceso transparente a los datos con fines de investigación (7).

Este cambio de paradigma introducido por el RGPD en los proveedores de servicios también ha brindado a los particulares la oportunidad de monetizar sus datos médicos vendiéndolos a investigadores médicos o empresas tecnológicas. De forma similar a Airbnb, que permitió a los particulares monetizar sus alojamientos libres, los pacientes, con su nueva propiedad y otros derechos otorgados por el GDPR, pueden ahora monetizar sus datos sanitarios personales a través de un "Mercado Digital de Datos Sanitarios" (DHDM) utilizando un modelo económico compartido. La figura 1 ilustra el flujo de trabajo operativo del DHDM. Sin embargo, con el actual marco centralizado de gestión de datos, en el que las HCE están fragmentadas en diferentes servicios cuando las normativas difieran entre organizaciones y jurisdicciones geográficas, será difícil gestionar el acceso y la administración, especialmente las microtransacciones en un entorno tan distribuido. En este contexto, blockchain y los contratos inteligentes asociados se consideran una tecnología revolucionaria, con una arquitectura distribuida incorporada y la capacidad de administrar la gobernanza de la información de forma descentralizada para distintos tipos de servicios digitales basados en transacciones.

El resto del documento está organizado de la siguiente manera: en primer lugar, revisamos 36 documentos relativos a los retos técnicos, centrándonos en tres áreas como la propiedad de los datos y el control del acceso, la interoperabilidad de los datos y la seguridad de los datos. A continuación, revisamos siete artículos relativos a cuestiones jurídicas y, por último, nueve artículos relacionados con cuestiones socioeconómicas.

DESAFÍOS TÉCNICOS

PROPIEDAD DE LOS DATOS Y CONTROL DE ACCESO

¿A quién pertenecen los datos sanitarios? Una pregunta que siempre ha intrigado y creado debates desde una perspectiva técnica, jurídica y filosófica. Kostkova et al. han polemizado sobre el tema y se han preguntado si los datos sanitarios deberían estar abiertos a la investigación, en un intento de encontrar un equilibrio entre la privacidad de las personas y el valor de la investigación respaldada por datos sobre la vida de millones de personas en todo el mundo (7). Los autores concluían instando a los responsables políticos a nivel internacional a desarrollar un marco regulador que salvaguarde la información personal, limite las explotaciones comerciales y permita el uso de los datos para la investigación y el uso comercial.

Se ha trabajado mucho en la propuesta de herramientas y modelos de control de acceso basados en blockchain,

Citación: Blockchain en Sanidad Hoy 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

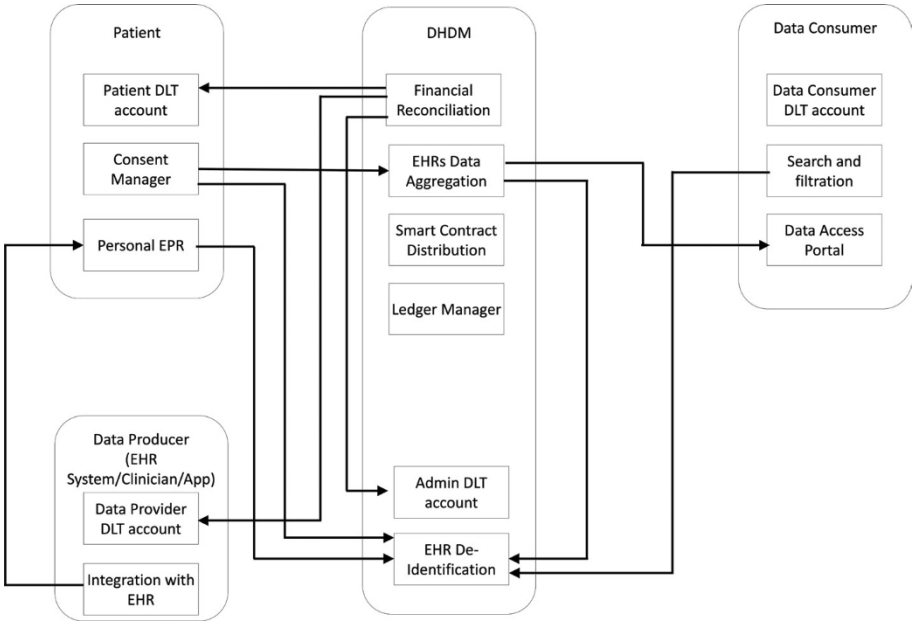

Figura 1. Cuatro interfaces del flujo de trabajo operativo de DHDM Cuatro interfaces del flujo de trabajo operativo de DHDM: A través de la interfaz del paciente (arriba a la izquierda), el paciente crea sus cuentas, completa su historia clínica electrónica (HCE) y gestiona el control de acceso dando su consentimiento para compartir sus datos con los investigadores de su elección. A través de la interfaz del productor de datos (abajo a la izquierda), los cuidadores y otros productores de datos pueden crear sus cuentas y gestionar la vinculación de los pacientes a sus archivos locales a través del sistema informático del cuidador. Los investigadores crearán sus cuentas, buscarán conjuntos de datos, solicitarán acceso a los datos y efectuarán los pagos por los datos a los que accedan a través de la interfaz de consumidor de datos (arriba a la derecha). La administración back-end del mercado se llevará a cabo a través de la interfaz DHDM, EPR (expediente electrónico del paciente) y DLT (tecnologías de libro mayor distribuido).

que sitúa al paciente en el asiento del conductor y le da todo el control para conceder y denegar el acceso a parte o a la totalidad de su HCE. La mayoría de los estudios intentaban dar ese control al paciente para obtener beneficios clínicos y operativos. Sin embargo, los mismos modelos propuestos también pueden beneficiar al control de los datos desde la perspectiva de la gestión de activos. Bahar et al. ofrecen una revisión bibliográfica específica que abarca la mayor parte de los trabajos en este ámbito. En este estudio, los autores abarcan y analizan principalmente trabajos sobre la gestión de registros de identidad digital y la autosuficiencia de los datos de HCE (8). Elaboraron una lista de soluciones de datos sociales implementadas mediante contratos inteligentes de Ethereum y las compararon en función de los incentivos, el mercado de datos, la habilitación de PHR, el seguimiento descentralizado de activos, la aplicación web/móvil, IoT, la compatibilidad/interoperabilidad de EHR y la implementación de pruebas de concepto.

Como se ha comentado anteriormente, Nguyen presentó un modelo para el control de acceso seguro a la HCE almacenada en una configuración de sistema de archivos interplanetario (IPFS) (9). El modelo proponía un gestor de HCE basado en un contrato inteligente para administrar el acceso y las solicitudes de transacciones de datos, al tiempo que proporcionaba al paciente una aplicación móvil basada en una interfaz blockchain para ejercer sus derechos de control de acceso. Aunque este modelo podría ser una solución fascinante para hacer frente a la decen-tralización de la HCE y, al mismo tiempo, proporcionar herramientas seguras y trazables para el control de acceso a los datos y la pista de auditoría de entrada, todas las pruebas prácticas de esta configuración mostraron una latencia muy alta en la operación.

una latencia de funcionamiento muy elevada. Rifi et al. abordaron el mismo concepto de uso de blockchain para administrar trans-acciones en EHR(10). Los autores manejaron el control de datos adquiridos de dispositivos médicos personales y sensores y propusieron una DApp eHealth blockchain para controlar la lectura/escritura en la base de datos EHR siendo nube o IPFS.

Nortey et al. ofrecen otro ejemplo de propuesta de marco de blockchain para la gestión de la privacidad de las HCE, al dar a los pacientes el control sobre quién accede a sus HCE
(11). Los autores introdujeron un mecanismo de canalización que garantiza que los pacientes autorizan a las entidades de la red distribuida a acceder a su información. Otros adoptan un enfoque diferente, en el que los autores pretendían construir un modelo de consentimiento para compartir datos (12, 13). Propusieron un flujo de trabajo de transacciones y crearon contratos inteligentes de Ethereum basados en LUCE (14). A blockchain solution for monitoring data License accoUntability and ComplianceE y siguieron con la construcción de un modelo arquitectónico basado en el con-sentimiento y luego lo implementaron en conjuntos de datos D1NAMO (15) de 29 participantes. Además, se propone un enfoque semidescentralizado, ya que la red de cadenas de bloques por encargo se distribuye entre distintas organizaciones (13). Las reglas de control de acceso se codifican en contratos inteligentes que se distribuyen a través de la red blockchain. Guo et al. presentan el mismo camino, pero proponen una arquitectura híbrida Blockchain-Edge (16).

Los datos de HCE se almacenan en nodos de borde que imponen políticas de control de acceso basadas en atri-butos. Los autores utilizaron la blockchain Hyperledger Composer Fabric programada con contratos inteligentes y políticas de listas de control de acceso para evaluar el rendimiento midiendo el procesamiento de las transacciones y el tiempo de respuesta frente a intentos de recuperación no autorizados. Los experimentos mostraron que el sistema proporciona resultados en milisegundos, lo que lo hace adecuado para ser incorporado en marcos de control de acceso a datos de HCE en tiempo real y seguros. El resultado más significativo es que la implementación mostró consistencia sobre los diferentes tamaños en todos los ensayos. Este resultado indica que esta arquitectura podría ser el modelo más escalable presentado en la gestión del consentimiento de HCE.

Otros autores también han presentado modelos de cadena de bloques basados en atributos para lograr la confidencialidad, integridad y autenticación de los datos de los pacientes y, al mismo tiempo, permitir el intercambio de datos entre las partes interesadas (17-20). Seol et al. prepararon su estudio de tal forma que veían el modelo desde el punto de vista de diferentes responsables políticos y construyeron su modelo en dos etapas (control de acceso y firma digital), permitiendo que los contratos inteligentes impusieran cada regla política a su vez.
(20). Yang et al. (21). se basaron en el modelo basado en atributos de Wang et al. (17) y construyeron una demostración para medir el rendimiento, especialmente el cifrado y el tiempo de búsqueda, y demostraron que el tiempo era independiente del número de atributos.

Guang et al. proporcionaron un modelo que depende del proveedor de atención sanitaria para controlar las transacciones de la HCE (22). Lo interesante de este modelo es que los autores proponen una arquitectura que implementa la tecnología blockchain con el sistema de HCE existente. Teniendo en cuenta que un sistema EHR tiene que tener un sistema de acceso múltiple y que los proveedores de salud mantienen individualmente los registros según el diseño del proceso de los au-tores, el modelo dio a los proveedores responsabilidades primarias, incluyendo la creación, verificación y anexión de nuevos bloques. El diseño utiliza contratos inteligentes, donde esta arquitectura es independiente de cualquier plataforma específica de blockchain, y sus variaciones pueden aplicarse potencialmente a cualquier sistema de HCE.

INTEROPERABILIDAD DE DATOS

La interoperabilidad de los datos es uno de los retos críticos para la informática sanitaria debido a la naturaleza heterogénea de los datos y a la falta de estandarización en los diferentes sistemas de HCE.

MedRec (23) fue la base que utilizaron muchos investigadores en blockchain para intercambiar/transferir de forma segura datos de sistemas distribuidos a una HCE unificada de pacientes. MedRec publicó un libro blanco industrial que explica un modelo de blockchain de código abierto para gestionar la transferencia segura de entradas de datos de HCE desde sistemas de proveedores sanitarios a nodos de pacientes y viceversa. El objetivo es recopilar de forma segura los datos creados en un archivo local de pacientes en cualquier número de hospitales y agregarlos en un archivo consolidado bajo el control del paciente. Al ser de código abierto, animó a muchos investigadores a utilizarlo en implantaciones de prueba y, del mismo modo, animó a pilotos industriales a adoptar su modelo. Este modelo de libro blanco es uno de los pocos modelos de blockchain en la sanidad que se han implantado. El trabajo de Yang et al. es un ejemplo de desarrollo académico basado en el marco MedRec (24).

MedShare (25) es una de las primeras propuestas de modelos de control de intercambio de datos de HCE mediante blockchain. Los autores empezaron sugiriendo una capa de procesamiento para administrar el intercambio de información entre la infraestructura en la nube de los proveedores sanitarios existentes. Sin embargo, la simulación demostró que la latencia es relativamente alta y aumenta con el incremento del número de usuarios. MedBlock (26) es un modelo similar. En este caso, los autores propusieron utilizar entidades de cadena de bloques no tradicionales, como servidores de autenticación y autoridades de certificación, para proporcionar medios para emitir identidades y asegurar el material criptográfico, que se utilizará para cifrar todos los datos de la cadena de bloques. Aunque MedBloc se diseñó para adaptarse a la infraestructura de TI sanitaria de Nueva Zelanda, el investigador no pudo detectar ninguna singularidad que dificultara su implantación en otros lugares.

Xiaoguang et al. (27) presentaron una adaptación reciente del modelo MedRec. Esta vez el objetivo era proporcionar e implementar un esquema de intercambio de datos médicos resistente a las manipulaciones: un mecanismo de Prueba de Estado Delegada que actuara como mecanismo de consenso ligero y fiable. Los resultados del análisis demostraron que el esquema era satisfactorio y tenía un bajo coste computacional y de comunicación. Este esquema se ajusta perfectamente al ámbito de la investigación sobre el mercado de datos, con la salvedad de que se trata de un esquema sin pago.

Zhuang et al. (28) proporcionaron otro marco que difiere del modelo MedRec. Aunque su objetivo es el mismo, lograr un intercambio de información sanitaria centrado en el paciente, este marco se centraba en potenciar el control del paciente con herramientas. El marco creó entonces una DApp para el paciente en la que éste puede ajustar parámetros en los contratos inteligentes otorgando permisos, permitiendo puntos de contacto y gestionando solicitudes de acceso a través de módulos de vinculación y solicitud. Este marco ofrece características prácticas al sistema: un adaptador de cadena de bloques configurado para la comunicación, el envío/recepción de historiales médicos y la creación de una presentación gráfica para los usuarios con una interacción sencilla, dos capas de seguridad para garantizar que sólo se ejecutan las funciones de contratos inteligentes autorizados, minimizar el riesgo de violación de datos, hashing para la coherencia de los datos, segmentación de datos que permite el intercambio parcial de datos y selección de puntos de contacto para que los clínicos seleccionen el segmento de datos relevante para la especialidad.

SEGURIDAD DE LOS DATOS

Desidentificar el historial del paciente es fundamental para garantizar la privacidad y la seguridad. Esto debe abordarse en dos

Citación: Blockchain en Sanidad Hoy 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

dos frentes en paralelo. Uno es separar los parámetros identificables del paciente de los datos clínicos. La separación debe hacerse en las capas de aplicación, comunicación y almacenamiento. El otro es el de los propios datos clínicos. Por ejemplo, cualquier imagen DICOM (Digital Imaging and Communications in Medicine) contiene datos identificables como el nombre del paciente, su fecha de nacimiento o el organismo que lo ha remitido. Por lo tanto, la desidentificación y la anonimización deben llevarse a cabo antes de colocar los datos en una red de cadena de bloques inmutable.

Varias investigaciones adoptaron el modelo de almacenar la HCE en blockchain (29, 30) Este enfoque fue descartado con el tiempo por razones técnicas y legales. Técnicamente, esto se debió al tamaño del bloque y a la capacidad de almacenar una gran cantidad de datos en una cadena que se replica en muchos nodos. Desde el punto de vista jurídico, apenas cumple los requisitos del artículo 17 (6) del GDPR, relativo al derecho ampliamente conocido como derecho al olvido, ya que no es posible modificar o eliminar un registro una vez almacenado en la cadena. Uno de los estudios que adoptó el enfoque de la HCE en la cadena es el de Tang et al. (30). Naturalmente, no habría sido relevante para esta investigación. Sin embargo, los autores propusieron un modelo interesante para la autenticación mediante un esquema de firma basado en la identidad con múltiples autoridades para el sistema de HCE basado en blockchain. El esquema ofrece lo que podrían ser algoritmos eficientes de firma y verificación.

Un gran número de publicaciones han propuesto lo que se ha dado en llamar seguridad de HCE de blockchain asistida por la nube. Wang et al. (31) presentaron un protocolo de intercambio de HCE seguro y que preserva la privacidad asistido por la nube basado en una blockchain de consorcio. En otras palabras, la HCE se almacena en la nube mientras que los índices de HCE (mantenimiento de registros) se guardan en la blockchain. En su trabajo, los autores proponen un esquema de intercambio de HCE basado en blockchain con encriptación conjuntiva de búsqueda por palabra clave y reencriptación proxy condicional para realizar la seguridad de los datos y la preservación de la privacidad del intercambio de datos entre diferentes organizaciones médicas.

Además, Kim et al. (32) proporcionaron un modelo y una prueba simulada de un protocolo seguro para un sistema de HCE asistido en la nube que utiliza blockchain. Demostraron la seguridad del esquema propuesto frente a ataques de intermediario (MITM) y de repetición mediante una simulación de validación automatizada de protocolos y aplicaciones de seguridad en Internet (AVISPA). Del mismo modo, Vora et al. (33) propusieron un modelo que utiliza blockchain para mejorar la seguridad de las bases de datos de HCE. En este caso, los autores se basaron en contratos inteligentes de Ethereum para gestionar consen-sos, permisos, clasificaciones y servicios. El modelo parece prometedor y sugiere seis algoritmos para abordar la seguridad de las transacciones y la preservación de la privacidad. Sin embargo, el modelo ha demostrado que sería imposible ocultar por completo toda la información y mantener un sistema accesible e interoperable. un sistema accesible e interoperable. Sin embargo, al utilizar contratos inteligentes para separar la información, el modelo propuesto sigue ofreciendo una preservación significativa de la privacidad y la integridad de los datos. Además, con un contrato inteligente, se puede determinar el nivel de acceso a la información, pero en blockchain pública, la integración con el contrato inteligente es un reto y no es práctica.

Aunque se trata de un estudio húngaro, Magyar et al. (34) presentaron un modelo basado en la firma de blockchain que adopta la normativa estadounidense de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). El modelo utiliza contratos inteligentes y las innovaciones de la industria de la criptografía, firmas ciegas, multifirmas, firmas jerárquicas y otros procedimientos de seguridad que garantizan el acceso a la información. Al mismo tiempo, en la ruta, nadie puede leer ningún dato de texto abierto.

En los estudios anteriores se ha tratado la HCE como una única base de datos, ya sea local o almacenada en la nube, y se han analizado distintos enfoques del uso de blockchain para añadir, eliminar y modificar entradas en la HCE de forma segura. Sin embargo, una de l a s principales razones por las que blockchain se identifica como una tecnología potencial para aumentar la solidez de la HCE y sus transacciones relacionadas es que las HCE están descentralizadas por naturaleza. Un paciente típico tendrá diferentes HCE en atención primaria, secundaria y terciaria. Sólo estos tres niveles a lo largo de la vida de un paciente pueden generar decenas de miles de registros que deben combinarse para formar una HCE completa del paciente.

En cambio, Ayesha et al. (35) analizaron una arquitectura alternativa que también cuestionaba el principio del almacenamiento de HCE en la nube. Los autores sugirieron un marco que propone medidas para garantizar que el sistema aborde el problema del almacenamiento de datos, ya que utiliza el mecanismo de almacenamiento fuera de la cadena del IPFS. El artículo evalúa el rendimiento de las distintas topologías en cuanto a tiempo de ejecución, rendimiento y latencia. Propone un marco que combina el almacenamiento seguro de registros con reglas de acceso a la cadena de bloques para las HCE.

Otro modelo de Nguyen et al. (9) se centra en el control de acceso seguro a la HCE y propone una configuración IPFS (InterPlanetary File System) para el almacenamiento de la HCE. La idea es formar un nodo IPFS en cada proveedor de asistencia y crear un gestor de HCE (servidor) que desempeñará el papel que inicialmente desempeñaba la HCE en la nube. A continuación, el modelo utiliza blockchain para indexar el rastro de las transacciones y tratar con el gestor de HCE como servicio en la nube. Internamente, el gestor de HCE es responsable de agregar el historial del paciente de todos los nodos IPFS a petición y crear más nodos a medida que el paciente se desplaza entre diferentes proveedores de atención. El modelo sugiere que el propio gestor de la HCE se base en un contrato inteligente para administrar las solicitudes de acceso y transacciones de datos, al tiempo que proporciona al paciente una aplicación móvil con interfaz de cadena de bloques para ejercer sus derechos de control del acceso.

RETOS JURÍDICOS Y ÉTICOS

La discusión jurídica siempre empieza por quién es el propietario de los datos. La propiedad se confunde a menudo con el acceso. Kostkova et al. (7) pretenden distinguir entre la propiedad de los datos y el derecho de acceso y encontrar nuevos enfoques equilibrados para satisfacer los intereses empresariales e implicar activamente al público, garantizando al mismo tiempo un acceso transparente a los datos para las necesidades de la investigación y las integraciones a gran escala que preserven la privacidad individual. Un estudio de Castillo et al. (36) trata de identificar los obstáculos al intercambio de información en el contexto de la Ley HITECH (Health Information Technology for Economic and Clinical Health) para crear un sistema sanitario más eficiente y eficaz. Los resultados sugieren que es más probable que un hospital intercambie resúmenes clínicos con hospitales de fuera de su sistema sanitario cuando el otro hospital utiliza el mismo proveedor de HCE. Los autores destacan la importancia de la neutralidad del proveedor de HCE y de ahí la importancia de la interoperabilidad de los sistemas de HCE.

En un estudio crítico de Yadav et al. (37) sobre la extracción de datos clínicos de las HCE de los pacientes, los autores exploran, discuten y presentan nuevas perspectivas sobre cómo se han utilizado las técnicas de extracción de datos para las HCE. En esta revisión sistemática, discuten la aplicación, el diseño del estudio y la metodología de minería de datos de un gran número de iniciativas para la minería de datos clínicos. Además, los autores discuten la barrera para el uso generalizado de la minería de datos en la práctica clínica. La revisión en sí no cubre las necesidades legales y regulatorias del DHDM. Sin embargo, aborda la ética y el cumplimiento de la investigación en minería de datos (IA, ML, etc.) facilitada a través del DHDM.

Mello Michellem presentó un manual exhaustivo sobre las barreras al crecimiento del intercambio de datos sanitarios en el contexto de las leyes norteamericanas (38). Los autores analizaron los estatutos y reglamentos federales y estatales sobre privacidad de la información sanitaria, así como material secundario, y concluyeron que persisten algunas barreras legales críticas, pero muchas cuestiones que los profesionales sanitarios reconocen como obstáculos son en cierto modo ilusorias. Los autores hicieron hincapié en que los profesionales sanitarios consideran que las leyes sobre privacidad de la información sanitaria obstaculizan el crecimiento del intercambio electrónico de datos sanitarios y culparon a varios factores, como la incoherencia de las leyes de consentimiento de los pacientes, el tratamiento especial de los datos sanitarios sensibles y la falta de establecimiento de un sistema unificado de indexación de pacientes.

Un documento tecno-normativo compara las diferencias entre las normas de transmisión de datos sanitarios (ISO/IEEE 11073, IHE PCD-01 y HL7 DoF) y sugiere el entorno más adecuado para utilizar cada una de ellas (39). Los autores concluyen que los mensajes ISO/IEEE 11073 no pueden contener información sobre el paciente, los mensajes IHE PCD-01 tienen información limitada sobre el dispositivo, y que HL7 DoF tiene la cobertura de información más completa en los cuatro parámetros del estudio (legibilidad humana, facilidad de aprendizaje, implementación y extensibilidad).

RETOS SOCIOECONÓMICOS

El término "destrucción creativa" acuñado por Joseph Schum-peter explica cómo el proceso de transformación de la industria revoluciona la estructura económica desde dentro destruyendo la existente y creando simultáneamente una nueva (40). Con tecnologías disruptivas como la cadena de bloques e industrias como la sanitaria, la estructura es extremadamente complicada en términos de compromisos de las partes interesadas e impulsos económicos.

Aunque no es médico, el modelo presentado por un estudio (41) proporcionaron una prometedora implementación de mercado basada en un modelo existente utilizado para el mercado de datos de vehículos comerciales de Japón. ID-Link fue un modelo exitoso cuando el gobierno de Japón inició la construcción de una infraestructura de información para compartir datos en diferentes áreas de negocio. Una de estas áreas era compartir datos de HCE individuales. En su trabajo, los autores sustituyen datos automovilísticos como velocidad, tiempo, autonomía, emisiones, etc. por datos médicos procedentes de la HCE. El estudio analizaba las opciones de compromiso (Opt-In vs. Opt-Out), los privilegios de control de acceso y la estandarización de datos, especialmente la adopción de formatos específicos como HL7 (el documento sugería V2.5., sin embargo, FHIR HL7-V3.0 se utiliza actualmente de forma generalizada en todo el mundo), CIE-10 de la OMS y SNOMED-CT como biblioteca de terminología clínica. El documento también ofrece una adaptación médica al flujo de trabajo del proceso au-tomotivo ID-Link en un modelo factible de siete pasos, desde el consentimiento del paciente, la interacción con el médico, la comprobación de la identidad, el uso comercial, el pago y la participación en los beneficios. El ID-Link se construye en cuatro capas arquitectónicas: empresarial, funcional, de datos y tecnológica.

Guo et al. (42) critican los procesos que siguen los innovadores en salud digital para extraer resultados de sus soluciones e implementaciones. Los autores también hacen hincapié en la falta de aplicación de las soluciones sanitarias digitales, por lo que no es fácil obtener resultados basados en pruebas. El estudio analiza algunas de las principales implantaciones de soluciones sanitarias digitales en función de una selección no exclusiva de normas reguladoras pertinentes y de las metodologías que los innovadores adoptaron para evaluar sus soluciones. No obstante, los autores reconocen que los innovadores no crean barreras y que se encuentran atrapados en la paradoja de "sin evidencia, no hay implementación; sin implementación, no hay evi-dencia" en salud digital. Los autores sugieren que enfoques como la investigación basada en la simulación pueden generar pruebas de mayor calidad, menor coste y más oportunas.

La encuesta de Affinito et al. (43), por el contrario, pretende conocer los medios digitales que utilizan los médicos para relacionarse con sus pacientes y el efecto que perciben los médicos en los resultados sanitarios clínicos. Los resultados de la encuesta sugieren que los principales factores de éxito para lograr la capacitación de los pacientes con herramientas digitales y mejorar los resultados sanitarios son las pruebas clínicas y la participación real de los usuarios (pacientes y cuidadores) en el diseño de las soluciones digitales. El estudio

Citación: Blockchain en Sanidad Hoy 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

concluye que el uso de herramientas digitales mejoraría la capacitación de los pacientes. Sin embargo, hasta la fecha, no hay pruebas de una mejora de los resultados sanitarios.

Una vez establecido que no hay pruebas que demuestren que los resultados de los pacientes mejoran con la adhesión al uso de herramientas digitales, Angeline y Sharon (44) realizaron un estudio para investigar si hay que culpar al nivel de alfabetización digital del personal sanitario. Este estudio demostró que la mayoría del personal mostraba confianza en el uso de las TIC. Sin embargo, se entiende que la ubicación del estudio (Australia) podría haber afectado a los resultados del mismo y que deberíamos anticipar otros resultados en otros territorios. Electronic Health Records for Clinical Research EH-R4CR es un proyecto europeo que pretendía mejorar los ensayos centrados en el paciente mediante el desarrollo de una plataforma que permite acceder a la HCE de los pacientes existentes (45), lo que hace que el proyecto sea muy similar al proyecto de investigación DHDM. Salvo que no se ocupa de la compensación al paciente por el uso de sus datos de HCE. Dupont et al. (46) es un estudio que evalúa los resultados financieros del proyecto. El estudio comparó EHR4CR con las prácticas existentes y concluyó que las soluciones EHR4CR parecen ahorrar costes a los patrocinadores principales de los ensayos clínicos. Los resultados del estudio sugieren que el potencial de ahorro aumentaría con una adopción más amplia de las soluciones EHR4CR en Europa y fuera de ella. Los resultados, a su vez, sugieren que un mercado de datos médicos en el que los pacientes puedan vender el acceso a sus registros de HCE para su propio beneficio ahorraría a largo plazo costes en ensayos industriales y clínicos.

En un artículo, Timo y Harri (47) intentaron desarrollar un Marco de Evaluación del Ecosistema (EEF) para comprender las posibilidades de supervivencia de una plataforma empresarial digital. Los autores describieron el modelo EEF en seis parámetros (la plataforma, el problema que la plataforma intenta reducir, el propósito de la plataforma, el ecosistema, las transacciones que permite la plataforma y el modelo de ingresos de la plataforma). Los autores destacan la importancia de tener en cuenta el modelo de compensación, que se ajusta perfectamente a los objetivos de nuestro estudio. Relacionan la omisión del componente de incentivos con la principal razón del fracaso del sistema regional de información sanitaria RHIS para alcanzar masas críticas en la región finlandesa de Pirkanmaa, donde aplicaron su modelo.

Alina y José Luis (48) analizaron lo que los autores denominaron un mercado FAIR. Identificaron los atributos para que los datos sean Localizables, Accesibles, Interoperables y Reutilizables, y de ahí surgió FAIR. Los au-tores presentaron una arquitectura que acomoda capas para reunir información de pacientes, proveedores de cuidados y otras plataformas como EHR4CR.

La puntuación crediticia siempre ha sido el mayor obstáculo para la investigación del DHDM. En casi todas las encuestas, sondeos o incluso charlas amistosas se ha planteado esta cuestión. La gente se pregunta si el proyecto les dejará tan expuestos como la puntuación crediticia a sus finanzas. A la gente siempre le preocupa que le denieguen o pague más por servicios que ahora obtiene sin estar muy expuesta al historial sanitario, como renovar el seguro del automóvil. Les preocupa que les suban las primas cuando la aseguradora conozca más detalles sobre su salud o, peor aún, que les denieguen servicios si no permiten el acceso a sus historiales, como ocurre con la puntuación crediticia.

Sin embargo, la arquitectura de la calificación crediticia es un ejemplo perfecto de agregación de datos y uso compartido autorizado desde una perspectiva tecno-comercial. Dumitru y Gatti (49) analizaron las limitaciones y las oportunidades relacionadas con la puesta en común de datos sanitarios y el uso de los datos con fines de calificación crediticia. Los autores han propuesto una arquitectura para un mercado de datos de confianza que puede ser muy útil para actuar como sistema de ponderación en el proyecto DHDM. El sistema de ponderación es lo que calcula la contribución de cada HCE a un conjunto de datos completo. Se utilizará para distribuir equitativamente los pagos de los investigadores médicos entre los propietarios de los datos de forma que se incentive la HCE en función de su compromiso con el bienestar y su compromiso de mantener la HCE actualizada.

Un estudio realizado por Roman y Stefano (50) es un ejemplo práctico de capitalización del exitoso modelo de puntuación crediticia en el cálculo del peso/valor de cada entrada de la HCE. El componente de ponderación tiene un enorme valor en una distribución justa de la riqueza entre los propietarios de HCE basada en la contribución de cada entrada y cada HCE en la investigación a la que se ha pagado la riqueza.

El estudio de Ryuji (41) es otro ejemplo práctico que podría beneficiar al proyecto de investigación DHDM. Proporciona un modelo viable de intercambio comercial de fondos contra datos que capitaliza técnicas ya aplicadas en la industria del automóvil.

CONCLUSIONES

Aunque se invierten miles de millones de dólares en hacer más eficientes los actuales sistemas de gestión de datos sanitarios, el intercambio de datos sigue siendo un objetivo difícil de alcanzar en el sector sanitario. Dado que el GDPR ha introducido un cambio de paradigma en la propiedad y el control de los datos, junto con las tecnologías similares a blockchain, que proporcionan la capacidad tecnológica de la gestión descentralizada de datos, es el momento adecuado para cambiar el modelo de incentivación sin desincentivos a través de un modelo de mercado abierto similar a DHDM.

Sobre la base de esta revisión, es evidente que las soluciones basadas en blockchain como MedRec (23) pueden implementarse como una capa independiente e integrarse con bases de datos nativas a través de interfaces de programación de aplicaciones (API) sin alterar los sistemas y la cultura de gestión de datos nativos, lo que sin duda beneficiará el proceso de adaptación de la tecnología. Además, al ser de código abierto, las soluciones similares a MedRec desempeñarán un papel importante en la recopilación segura de datos a partir de los sistemas de gestión de datos existentes y en la combinación de las tecnologías de la información y la comunicación.

una HCE agregada bajo el control del paciente. Los contratos inteligentes y los sistemas IPFS/de almacenamiento en la nube proporcionarán a los pacientes el control para conceder de forma segura el acceso a diferentes tipos y duración de datos desidentificados. La revisión demostró diferentes propuestas para el acceso a los datos y su intercambio seguro entre productores y consumidores de datos. Sin embargo, es necesario realizar más estudios sobre la reproducción de datos digitales y cómo garantizar los derechos del productor si el consumidor reproduce los datos sin su consentimiento. También son necesarios más estudios para determinar cómo adaptar el proceso de intercambio de datos a las distintas normativas de las distintas jurisdicciones geográficas y temporales.

También es necesario evaluar exhaustivamente el modelo de incentivación basado en la economía compartida que se considere más apropiado para el contexto de DHDM. Aunque una empresa como Airbnb tiene beneficios económicos demostrables tanto para el proveedor como para el consumidor, compartir datos sanitarios personales puede tener un contexto social y emocional diferente al del alojamiento personal. A pesar de estas preocupaciones, es casi seguro que un mercado abierto introducirá competencia para producir e impulso para compartir datos de alta calidad en función de la demanda de los consumidores. Esto, a su vez, facilitará a investigadores y médicos el acceso a los datos según sus necesidades.

Declaración de financiación

Este artículo no ha recibido financiación alguna.

Relaciones y actividades financieras y no financieras

Los autores declaran no tener ningún conflicto de intereses.

Contribuciones de los autores

Los dos autores del artículo han contribuido sustancialmente al trabajo. Mohamed Maher conceptualizó el modelo, realizó la revisión bibliográfica y redactó el artículo. Imtiaz Khan facilitó el diseño, redactó y formateó el artículo.

REFERENCIAS

1. Heather B. Google DeepMind y Royal Free en un acuerdo de cinco años. Digitalhealth; 2016. Disponible en: https://www.digitalhealth.net/2016/11/google-deepmind-and-royal-free-in-five-year-deal/ [citado el 19 de septiembre de 2021].
2. Kowelle J. Los datos del NHS valen miles de millones, pero ¿quién debería tener acceso a ellos? The Guardian. 2019. Disponible en: https://www. theguardian.com/society/2019/jun/10/nhs-data-google-alpha-bet-tech- [citado el 19 de septiembre de 2021].
3. PatientsLikeMe. patientslikeme.com. 2021.
4. Jeana HF, Michael PM. Social uses of personal health informa-tion within PatientsLikeMe, an online patient community: What can happen when patients have access to one another's data. J Med Internet Res. 2008;10(3):e15. doi: 10.2196/jmir.1053
5. Paul W, Michael M, Jeana F, et al. Compartir datos sanitarios para obtener mejores resultados en PatientsLikeMe. J Med Internet Res. 2010;12(2):e19. doi: 10.2196/jmir.1549
6. GDPR. Reglamento general de protección de datos. Intersoft Consulting. 2016. Disponible en: https://gdpr-info.eu [citado el 19 de septiembre de 2021].
7. Kostkova P, Brewer H, de Lusignan S, et al. ¿A quién pertenecen los datos? Datos abiertos para la atención sanitaria. Front Public Health. 2016;4:7. doi: 10.3389/fpubh.2016.00007
8. Bahar H, Abdelhakim Senhaji H, Dimitrios M. A sur-vey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access. 2020;8:90478-94. doi: 10.1109/ access.2020.2994090
9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Block-chain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access. 2019;7:66792-806. doi: 10.1109/ ACCESS.2019.2917555
10. Rifi N, Rachkidi E, Agoulmine N, Taher NC. Hacia el uso de la tecnología blockchain para la gestión de acceso a datos de eHealth. IEEE; 2017, p. 1-4.
11. Nortey RN, Yue L, Agdedanu PR, Adjeisah M, editores. Módulo de privacidad para registros electrónicos de salud distribuidos(EHRs) utilizando el blockchain. 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), 15-18 de marzo de 2019.
12. Jaiman V, Urovi V. Un modelo de consentimiento para plataformas de intercambio de datos de salud basadas en blockchain. IEEE Access 2020;8:143734-45. doi: 10.1109/ACCESS.2020.3014565
13. Ryno A, Bertram H. Un enfoque de blockchain con permiso para el proceso de autorización en los registros electrónicos de salud. 2019 International Multidisciplinary Information Technology and En-gineering Conference (IMITEC). 2020.
14. Havelange A, Dumontier M, Wouters B, et al. LUCE: A blockchain solution for monitoring data License accoUnt-ability and ComplianceE. 2019. Disponible en: https://arxiv.org/ abs/1908.02287 [citado el 19 de septiembre de 2021].
15. Fabien D, Jean-Eudes R, Stefano B, Jean-Paul C, Juan R, Mi-chael S. El conjunto de datos abierto D1NAMO: A multi-modal dataset for research on non-invasive type 1 diabetes management. Informat Med Unlocked. 2018;13:92-100. doi: 10.1016/j.imu.2018.09.003
16. Guo H, Li W, Nejad M, Shen C, editores. Control de acceso para registros de salud elec-trónicos con arquitectura híbrida blockchain-edge. 2019 IEEE International Conference on Blockchain (Block-chain), 14-17 de julio de 2019.
17. Wang H, Song Y. Secure cloud-based EHR system using at-tribute-based cryptosystem and blockchain. J Med Syst. 2018;42(8):1-9. doi: 10.1007/s10916-018-0994-6
18. Guo R, Shi H, Zhao Q, Zheng D. Esquema seguro de sig-natura basado en atributos con múltiples autoridades para blockchain en sistemas de registros de salud elec-trónicos. IEEE Access. 2018;6:11676-86. doi: 10.1109/ACCESS.2018.2801266
19. Sun Y, Zhang R, Wang X, Gao K, Liu L, editores. A decentral-izing attribute-based signature for healthcare blockchain. 2018 27th International Conference on Computer Communication and Networks (ICCCN), 30 de julio-2 de agosto de 2018.
20. Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-preserv-ing attribute-based access control model for XML-based elec-tronic health record system. IEEE Access. 2018;6(99):9114-28. doi: 10.1109/ACCESS.2018.2800288
21. Yang X, Li T, Rui L, et al. Esquema de intercambio de ehr seguro y con capacidad de búsqueda basado en blockchain. 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 24-26 de octubre de 2019.
22. Guang Y, Chunlei L. Un diseño de arquitectura basada en blockchain para la seguridad de los sistemas de historia clínica electrónica (HCE). 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). 2018.

23. Azaria A, Ekblaw A, Vieira T, Lippman A, editores. MedRec: Using blockchain for medical data access and permission man-agement. 2016 2nd International Conference on Open and Big Data (OBD), 22-24 de agosto de 2016.
24. Yang H, Yang B, editores. A blockchain-based approach to the secure sharing of healthcare data. Actas de la Conferencia de Seguridad de la Información de Noruega; 2017.
25. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeD-Share: Intercambio de datos médicos sin confianza entre proveedores de servicios en la nube a través de blockchain. IEEE Access. 2017;5:14757-67. doi: 10.1109/ACCESS.2017.2730843
26. Huang J, Qi YW, Asghar MR, Meads A, Tu Y, editores. Med-Bloc: Un sistema EHR seguro basado en blockchain para compartir y acceder a datos médicos. 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 5-8 de agosto de 2019.
27. Xiaoguang L, Ziqing W, Chunhua J, Fagen L, Gaoping L. Esquema de protección e intercambio de datos médicos basado en blockchain. IEEE Access. 2019;7:118943-53. doi: 10.1109/ access.2019.2937685
28. Zhuang Y, hojas LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR. Un marco de intercambio de información de salud centrado en el paciente utilizando tecnología blockchain. IEEE J Biomed Health Informat 2020;24(8):2169-76. doi: 10.1109/JBHI.2020.2993072
29. Xu L, Bagula A, Isafiade O, Ma K, Chiwewe T, editores. Diseño de una plataforma de historiales médicos electrónicos basada en una cadena de bloques creíble (CB-EHRS). Caleidoscopio de la UIT 2019: TIC para la salud: Redes, normas e innovación (UIT K), 4-6 de diciembre de 2019.
30. Tang F, Ma S, Xiang Y, Lin C. Un esquema de autenticación eficiente para registros electrónicos de salud basados en blockchain. IEEE Access. 2019;7:41678-89. doi: 10.1109/ACCESS.2019.2904300
31. Wang Y, Zhang A, Zhang P, Wang H. Intercambio de HCE asistido por la nube con preservación de la seguridad y la privacidad a través de blockchain de consorcio. IEEE Access. 2019;7:136704-19. doi: 10.1109/ ACCESS.2019.2943153
32. Kim M, Yu S, Lee J, Park Y, Park Y. Diseño de proto-col seguro para sistema de historia clínica electrónica asistido en la nube usando blockchain. Sensors (Basilea, Suiza) 2020;20(10):2913. doi: 10.3390/s20102913
33. Vora J, Nayyar A, Tanwar S, et al., editores. BHEEM: Un marco basado en cadena de bloques para asegurar los registros electrónicos de salud. 2018 IEEE Globecom Workshops (GC Wkshps); 9-13 de diciembre de 2018.
34. Magyar G, editor. Blockchain: Solving the privacy and re-search availability tradeoff for EHR data: Una nueva tecnología disruptiva en la gestión de datos de salud. 2017 IEEE 30th Neu-mann Colloquium (NC); 24-25 de noviembre de 2017. doi: 10.1109/ NC.2017.8263269
35. Ayesha S, Usman Q, Ayesha K. Uso de blockchain para registros electrónicos de salud. IEEE Access. 2019;7:147782-95. doi: 10.1109/ access.2019.2946373
36. Castillo AF, Sirbu M, Davis AL. Vendor of choice and the effectiveness of policies to promote health information ex-change. BMC Health Serv Res 2018;18(1):405-12. doi: 10.1186/ s12913-018-3230-7
37. Yadav P. Minería de registros electrónicos de salud (EHR): Una encuesta. ACM Comput Surv. 2017;50(6):1-41. doi: 10.1145/3127881
38. Michellem M. Barreras legales para el crecimiento del intercambio de información sanitaria: ¿piedras o guijarros? Milbank Q 2018;96(1):110-44. doi: 10.1111/1468-0009.12313
39. Lee S, Do H. Comparación y análisis de los mensajes ISO/IEEE 11073, IHE PCD-01 y HL7 FHIR para dispositivos de salud personales. Healthc Inform Res. 2018;24(1):46-52. doi: 10.4258/ hir.2018.24.1.46
40. Schumpeter JA, Stiglitz JE. Capitalism, socialism and democ-racy (Capitalismo, socialismo y democracia). Florence, SC: Taylor & Francis Group; 2010.
41. Ryuji I. ID-link, an enabler for medical data marketplace. IEEE. 2016. doi: 10.1109/ICDMW.2016.0117
42. Guo C, Ashrafian H, Ghafur S, Fontana G, Gardner C, Prime M. Challenges for the evaluation of digital health solutions-A call for innovative evidence generation approaches. NPJ Digit Med. 2020;3(1):1-14. doi: 10.1038/s41746-020-00314-2
43. Affinito L, Fontanella A, Montano N, Brucato A. How physi-cians can empower patients with digital tools. J Public Health. 2020:1–13.doi: 10.1007/s10389-020-01370-4
44. Kuek A, Hakkennes S. Healthcare staff digital literacy levels and their attitudes towards information systems. Health Informatics J. 2020 Mar;26(1):592-612. doi: 10.1177/1460458219839613
45. EHR4CR | Sistemas de historias clínicas electrónicas para la reinvestigación clínica. Iniciativa sobre medicamentos innovadores. 2016. Disponible en: https://www.imi.europa.eu/projects-results/project-factsheets/ ehr4cr [citado el 19 de septiembre de 2021].
46. Dupont D, Beresniak A, Schmidt A, Proeve J, Bolanos E. Assessing the financial impact of reusing electronic health re-cords data for clinical research: Results from the EHR4CR European project. J Health Med Informat. 2016;7(3):235. doi: 10.4172/2157-7420.1000235
47. Timo I, Harri T. Modelos de negocio difíciles de plataformas empresariales digitales para datos sanitarios: Un marco para la evaluación de la viabilidad del ecosistema. 2017 IEEE 19th Conference on Business In-formatics (CBI); 2017. doi: 10.1109/cbi.2017.6
48. Alina T, José Luis O. Un mercado FAIR para custodios de datos biomédicos e investigadores clínicos. 2018 IEEE 31st In-ternational Symposium on Computer-Based Medical Systems (CBMS); 2018. doi: 10.1109/cbms.2018.00040
49. Dumitru R, Gatti S. Hacia una arquitectura de referencia para mercados de datos de confianza: La perspectiva de la calificación crediticia. 2016 2nd In-ternational Conference on Open and Big Data (OBD). 2016. doi: 10.1109/obd.2016.21
50. Roman D, Stefano G, editores. Hacia una arquitectura de referencia para los mercados de datos de confianza: La perspectiva de la calificación crediticia. 2016 2nd International Conference on Open and Big Data (OBD); 22-24 de agosto de 2016. doi: 10.1109/OBD.2016.21