(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 698**

(51) Int. CI.:

***G16H 10/65*** (2008.01)
***G06F 21/62*** (2013.01)
***H04L 9/14*** (2006.01)
***H04L 9/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.03.2016 PCT/US2016/020388**

(87) Fecha y número de publicación internacional: **09.09.2016 WO16141029**

(96) Fecha de presentación y número de la solicitud europea: **02.03.2016 E 16759392 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3266149**

(54) Título: **Control de acceso para datos encriptados en identificadores legibles por máquina**

(30) Prioridad:

**03.03.2015 US 201562127404 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**05.03.2021**

(73) Titular/es:

**WONDERHEALTH, LLC (100.0%)**
**P.O. Box 17498**
**Atlanta, GA 30316, US**

(72) Inventor/es:

**HILL, KENNETH y**
**HILL, KATHERINE, S.**

(74) Agente/Representante:

**SUGRAÑES MOLINÉ, Pedro**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Control de acceso para datos encriptados en identificadores legibles por máquina

**Referencia cruzada a solicitudes relacionadas**

Esta solicitud reivindica el beneficio y la prioridad de la solicitud de Patente Provisional de Estados Unidos N.º 62/127.404, en trámite, titulada "GENERATING IDENTIFIER WITH ENCODED HEALTH INFORMATION", presentada el 3 de marzo de 2015.

**Antecedentes**

Los identificadores legibles por máquina pueden emplearse para formatear datos en un medio reconocible por un dispositivo lector, tal como un escáner de código de barras o de código de matriz. Sin embargo, cualquier persona que tiene un lector adecuado puede obtener los datos incorporados en el identificador legible por máquina a no ser que los datos subyacentes estén encriptados. Gestionar qué dispositivos tienen acceso a datos encriptados en identificadores legibles por máquina sigue siendo problemático.

El documento US 2006/088166 A1 se refiere a autenticación y distribución de información secreta entre dispositivos que realizan una comunicación inalámbrica de corto alcance. Cuando un dispositivo que incluye una unidad de comunicación inalámbrica de corto alcance, una unidad de creación de código de barras, una unidad de lectura de código de barras y una unidad de análisis de código de barras se conecta a un dispositivo que incluye una unidad de comunicación inalámbrica de corto alcance, una unidad de creación código de barras, una unidad de lectura de código de barras y una unidad de análisis de código de barras para realizar la comunicación inalámbrica de corto alcance, se realiza una interacción de tal manera que información de seguridad tal como una clave de autenticación y una clave de encriptación se convierte a un código de barras, para su reconocimiento por la otra parte. Se realiza la autenticación de la otra parte a través de la interacción usando este código de barras, y también se distribuye la clave de encriptación a usarse para la comunicación inalámbrica de corto alcance posterior.

El documento US 8.690.062 B2 divulga que almacenar un evento desde una fuente impresa en un calendario electrónico puede incluir un ID de evento con código de barras en la fuente impresa. Una fuente impresa puede ser cualquier visualizador visual no interactivo. El ID de evento puede ser en forma de un código de barras impreso en matriz o lineal y puede incluir información codificada tal como, pero sin limitación, hora y fecha de evento y ubicación de evento. Opcionalmente, el ID de evento también puede incluir información tal como un nombre de contacto de evento e información de contacto, así como un posible método de RSVP y dirección. El ID de evento puede ser en lugar de información de texto especial o alfanumérica escrita comúnmente o legible por humanos. En otra realización, el ID de evento puede encriptarse requiriendo que un individuo tenga una clave de desencriptado para acceder a la información de evento.

El documento US 2008/149701 A1 divulga un aparato y método para producir y visualizar un código de barras dinámico que permite que personal médico autorizado obtenga información médica confidencial mientras evitan que personal no autorizado vea la misma. Cualquier información médica dinámica adecuada puede visualizarse de esta manera, incluyendo presión sanguínea, temperatura, frecuencia respiratoria, frecuencia cardiaca y similares.

**Campo de la invención**

La presente divulgación se refiere a criptografía, tecnología de identificador legible por máquina, seguridad de datos y, en cierto grado, visión informática.

**Breve descripción de los dibujos**

Muchos aspectos de la presente divulgación pueden entenderse mejor con referencia a los siguientes dibujos. Los componentes en los dibujos no están necesariamente a escala, con énfasis en su lugar situándose en ilustrar claramente los principios de la divulgación. Además, en los dibujos, números de referencia similares designan correspondientes partes a través de las varias vistas.

La Figura 1 muestra un ejemplo de un entorno en red para proporcionar control de acceso a información recopilada por una aplicación cliente según diversas realizaciones.
La Figura 2 muestra otro ejemplo de un entorno en red para aumentar y actualizar datos de contenido usando identificadores legibles por máquina encriptados según diversas realizaciones.
La Figura 3 muestra una estructura de datos usada para generar un identificador legible por máquina que tiene porciones de datos encriptados usando múltiples claves según diversas realizaciones.
La Figura 4 incluye una tabla que ilustra la capacidad de un código de matriz de versión 40-L.
La Figura 5 incluye una tabla que ilustra los bits de indicador de modo para un modo de codificación de datos.
La Figura 6 es un diagrama de flujo que ilustra un ejemplo de encriptación y codificación de datos para su uso en un identificador legible por máquina según diversas realizaciones.

Las Figuras 7A-7N muestran diversos ejemplos de interfaces de usuario generadas por una aplicación cliente según diversas realizaciones.

La Figura 8 es pseudocódigo que ilustra un ejemplo de código usado para configurar un dispositivo informático o un dispositivo cliente para generar un identificador legible por máquina según diversas realizaciones.

La Figura 9 muestra un ejemplo de actualización o aumento de datos en un dispositivo cliente usando un identificador legible por máquina generado por otro dispositivo según diversas realizaciones.

Las Figuras 10-12 son diagramas de flujo que ilustran una funcionalidad de una aplicación cliente ejecutada en un dispositivo cliente según diversas realizaciones.

Las Figuras 13 y 14 son diagramas de flujo que ilustran una funcionalidad de una aplicación remota ejecutada en un entorno informático según diversas realizaciones.

Las Figuras 15-17 son diagramas de bloque esquemáticos que proporcionan ilustraciones de ejemplo de un entorno informático, un dispositivo cliente y un dispositivo lector empleados en el entorno en red de las Figuras 1 y 2 según diversas realizaciones.

**Descripción detallada**

La presente divulgación se refiere a control de acceso para datos segmentados en identificadores legibles por máquina. Los identificadores legibles por máquina, tal como códigos de barras, códigos de matriz u otros identificadores similares, pueden emplearse para formatear datos en un medio reconocible por un dispositivo lector, tal como un código de barras o un escáner de código de matriz. Mientras identificadores legibles por máquina pueden usarse para transferir datos desde un dispositivo a otro sin el uso de una red por cable o inalámbrica, cualquier persona que tiene un lector adecuado puede obtener los datos incorporados en el identificador legible por máquina a no ser que los datos subyacentes estén encriptados. Ya que los datos subyacentes pueden ser sensibles, un usuario puede querer controlar qué porciones de los datos subyacentes se pueden leer por diversos dispositivos.

Por ejemplo, en algunas realizaciones, la información médica puede codificarse en un identificador legible por máquina. A veces se requiere que las personas produzcan datos sensibles que la persona puede desear mantener privados, tal como proporcionar un historial médico durante una visita a una consulta médica. El historial médico, así como otra información de identificación personal, se requiere generalmente por quiroprácticos, proveedores de medicina holística, veterinarios, centros médicos de emergencias o urgencias, dentistas, compañías de seguros, *etc.* Los miembros de la familia pueden soportar la responsabilidad de proporcionar tal información a proveedores de asistencia sanitaria en nombre de sus parientes si estos no son capaces de hacerlo.

Mientras una persona puede querer proporcionar a su médico de cabecera con un historial médico completo, la persona puede no querer proporcionar el historial médico completo a otro proveedor, tal como un quiropráctico o un dentista. En su lugar, pueden desear limitar los datos a lo que es relevante para el profesional de la atención sanitaria. Por consiguiente, en diversas realizaciones, un único identificador legible por máquina puede codificarse con datos en los que diferentes dispositivos son capaces de leer diferentes porciones de los datos. Por ejemplo, una persona puede autorizar a su médico de cabecera para obtener un historial médico completo a partir de un código de matriz mientras un quiropráctico, usando el mismo código de matriz, puede ser capaz únicamente de obtener un subconjunto del historial médico como autorizado por un usuario.

Según diversas realizaciones, un usuario puede usar su dispositivo electrónico, tal como un teléfono inteligente o tableta, para proporcionar información de admisión médica, al contrario que la práctica habitual de rellenar formularios médicos usando lápiz y papel. Ya que la información médica, personal u otra información proporcionada por el usuario a través del dispositivo electrónico puede ser sensible, enviar la información a través de una red plantea preocupaciones. Por ejemplo, la información podría interceptarse usando software de rastreo de paquetes o puntos de acceso maliciosos. Además, las bases de datos en las que la información se almacena pueden piratearse. Como tal, pueden usarse identificadores legibles por máquina, tales como códigos de barra o códigos de matriz, para transferir información entre dispositivos cercanos sin el uso de una red.

Los identificadores legibles por máquina, sin embargo, normalmente se basan en normas de código abierto o transparentes que hacen que la interpretación de datos incorporados en los identificadores legibles por máquina sea susceptible de acceso no autorizado. Por ejemplo, si la información médica se embebió en un código de matriz, cualquier lector de código de matriz comercialmente disponible puede ser capaz de obtener la información médica. Mientras los datos subyacentes pueden encriptarse, únicamente dispositivos que tienen acceso a una clave adecuada pueden desencriptar los datos. Sin embargo, compartir una única clave entre múltiples dispositivos disuade a una persona de proporcionar una cantidad completa de información ya que la persona puede ser consciente de que todos dispositivos con la clave son capaces de acceder a su información.

Por consiguiente, en realizaciones descritas en este documento, puede proporcionarse control de acceso para datos segmentados en identificadores legibles por máquina. En una realización, una aplicación cliente ejecutable en un dispositivo cliente puede configurarse para recibir una primera clave criptográfica asociada con un primer perfil de dispositivo y una segunda clave criptográfica asociada con un segundo perfil de dispositivo a través de una red. La aplicación cliente puede facilitar la recopilación de datos de entrada de un usuario a través de un proceso de ingestión que puede incluir una serie de interfaces de usuario que avisan al usuario para que introduzca una

diversidad de datos. Una vez recibidos, la aplicación cliente puede segmentar o formatear de otra manera los datos de entrada en al menos una primera porción de datos y una segunda porción de datos. Por ejemplo, la primera porción de datos puede ser capaz de interpretarse por un dispositivo lector para un médico de cabecera mientras la segunda porción de datos puede ser capaz de interpretarse por un dispositivo lector para un quiropráctico.

La aplicación cliente puede encriptar la primera porción de datos usando la primera clave criptográfica y la segunda porción de datos usando la segunda clave criptográfica. Una aplicación remota, denominada en este documento como una aplicación de gestión de clave, puede ejecutarse en un dispositivo informático remoto, tal como un servidor, y supervisar la transmisión y recepción de claves capaces de desencriptar los datos, según se autorice por el usuario. Como alternativa, en otras realizaciones, un dispositivo receptor puede asociarse con una clave en el entorno informático remoto. La aplicación remota puede proporcionar a la aplicación cliente una clave para un dispositivo receptor, de tal forma que la información se encripta para su acceso por el dispositivo receptor. Finalmente, la aplicación cliente puede generar un identificador legible por máquina usando la primera porción de datos encriptados y la segunda porción de datos encriptados para representar en un visualizador accesible por el dispositivo cliente. El dispositivo receptor puede capturar una o más imágenes del identificador legible por máquina para acceder a los datos subyacentes usando análisis de imágenes automatizado y visión informática.

Como un ejemplo no limitante, un usuario de la aplicación cliente puede asociar su médico de cabecera con un alto nivel de acceso, en el que el médico de cabecera es capaz de usar su dispositivo para acceder a todos los datos de entrada proporcionados por el usuario de la aplicación cliente. La aplicación de gestión de clave puede enviar una clave al dispositivo para el médico de cabecera, así como al dispositivo para el usuario. De manera similar, la aplicación de gestión de clave puede enviar una clave al dispositivo para el quiropráctico u otro proveedor médico y al dispositivo para el usuario. La aplicación cliente puede codificar datos autorizados para su recepción por el médico de cabecera usando una correspondiente clave mientras codifica datos autorizados para su recepción por el quiropráctico usando una clave diferente para el quiropráctico. Para este fin, usando un único identificador legible por máquina, se proporciona control de acceso a los datos subyacentes del identificador legible por máquina.

Como puede apreciarse, existe un problema técnico para transferir datos sensibles entre dispositivos sin el uso de una red ya que existen muchas formas de interceptar datos transmitidos a través de una red. Adicionalmente, existe un problema técnico de que existen muchas formas en las que pueden obtenerse datos almacenados de red (datos almacenados en un dispositivo de red) sin autorización. Por consiguiente, las realizaciones descritas en este documento resuelven el problema técnico presentando formas de transmitir datos sensibles entre dispositivos sin el uso de la red para transmitir y recibir los datos sensibles.

Aunque esta divulgación proporciona múltiples ejemplos en el contexto de datos de atención sanitaria, las realizaciones adjuntas en este documento son aplicables a través de muchas industrias. Adicionalmente, esta divulgación proporciona ejemplos en el contexto de códigos de matriz y otros identificadores similares legibles por máquina. Sin embargo, en algunas realizaciones, puede emplearse reconocimiento de imagen visual para identificar datos codificados en diferentes formas de imágenes, tales como los empleados en las aplicaciones de Clickable Paper™ comercializadas por RICOH®.

En la siguiente descripción, se proporciona una descripción general del sistema y sus componentes, seguida por una descripción de la operación del mismo.

Con referencia a la Figura 1, se muestra un entorno en red 100 según diversas realizaciones. El entorno en red 100 incluye un entorno informático 103, un dispositivo cliente 106 y un dispositivo lector 109, que están en comunicación de datos entre sí a través de una red 112. En diversas realizaciones, el dispositivo cliente 106 y el dispositivo lector 109 pueden no comunicar ninguna información desde un dispositivo a otro a través de la red 112 más allá de claves criptográficas, como se analizará. La red 112 incluye, por ejemplo, la Internet, intranets, extranets, redes de área extensa (WAN), redes de área local (LAN), redes por cable, redes inalámbricas u otras redes adecuadas, *etc.,* o cualquier combinación de dos o más de tales redes. Por ejemplo, tales redes pueden comprender redes por satélite, redes de cable, redes de Ethernet y otros tipos de redes.

El entorno informático 103 puede comprender, por ejemplo, un ordenador de servidor o cualquier otro sistema que proporciona capacidad de cálculo. Como alternativa, el entorno informático 103 puede emplear una pluralidad de dispositivos informáticos que pueden disponerse, por ejemplo, en uno o más bancos de servidores, bancos de ordenadores u otras disposiciones. Tales dispositivos informáticos pueden ubicarse en una única instalación o pueden distribuirse entre muchas diferentes localizaciones geográficas. Por ejemplo, el entorno informático 103 puede incluir una pluralidad de dispositivos informáticos que juntos pueden comprender un recurso informático alojado, un recurso informático en red y/o cualquier otra disposición informática distribuida. En algunos casos, el entorno informático 103 puede corresponder a un recurso informático elástico en el que la capacidad asignada de procesamiento, red, almacenamiento u otros recursos relacionados con ordenadores puede variar con el paso del tiempo.

Diversas aplicaciones y/u otra funcionalidad pueden ejecutarse en el entorno informático 103 según diversas realizaciones. También, diversos datos se almacenan en un almacenamiento de datos 115 que son accesibles para

el entorno informático 103. El almacenamiento de datos 115 puede ser representativo de una pluralidad de almacenamientos de datos 115 como puede apreciarse. Los datos almacenados en el almacenamiento de datos 115, por ejemplo, se asocian con la operación de las diversas aplicaciones y/o entidades funcionales descritas a continuación.

Los componentes ejecutados en el entorno informático 103, por ejemplo, pueden incluir una aplicación de gestión de clave 118, un servicio de traducción 120, un servicio de mensajería directa 122 y otras aplicaciones, servicios, procesos, sistemas, motores o funcionalidad no analizados en detalle en este documento. La aplicación de gestión de clave 118 puede ejecutarse para supervisar la transmisión y recepción de diversas claves criptográficas 121a...121c almacenadas en el almacenamiento de datos 115, como se analizará.

El servicio de traducción 120 puede ejecutarse para traducir una entrada de usuario desde un primer idioma, tal como español, a un segundo idioma, tal como inglés. En algunas realizaciones, el servicio de traducción 120 puede usarse para traducir una pregunta almacenada en el entorno informático 103 para su uso en un proceso de ingestión desde un primer idioma a un segundo idioma.

El servicio de mensajería directa 122 puede emplearse para enviar mensajes directos encriptados a través de la red desde un dispositivo cliente 106 a otro. En una realización, una aplicación ejecutable en el dispositivo cliente 106 encripta un mensaje generado por un usuario del dispositivo cliente 106 y envía el mensaje encriptado al servicio de mensajería directa 122 a través de la red 112 que, a continuación, transmite el mensaje encriptado a un dispositivo cliente receptor 106. En un ejemplo, el servicio de mensajería directa 122 permite que un paciente se comunique directamente con su proveedor sanitario. En otras realizaciones, pueden pasarse mensajes entre dispositivos cliente 106 usando un identificador legible por máquina, como se analizará.

En realizaciones adicionales, el entorno informático 103 puede incluir aplicaciones o servicios que proporcionan almacenamiento basado en la nube de información encriptada, tal como información de salud encriptada, aunque en otras realizaciones, la información encriptada puede no almacenarse en el entorno informático 103.

El dispositivo cliente 106 es representativo de una pluralidad de dispositivos cliente que pueden acoplarse a la red 112. El dispositivo cliente 106 puede comprender, por ejemplo, un sistema basado en procesador tal como un sistema informático. Un sistema informático de este tipo puede incorporarse en forma de un ordenador de sobremesa, un ordenador portátil, asistentes digitales personales, teléfonos celulares, teléfonos inteligentes, decodificadores de salón, reproductores de música, tabletas web, sistemas informáticos de tableta, consolas de juegos, lectores de libro electrónico, relojes inteligentes u otros dispositivos con capacidad similar. El dispositivo cliente 106 puede incluir un visualizador de dispositivo cliente 124 y el dispositivo lector 109 puede incluir un visualizador de dispositivo lector 127. El visualizador de dispositivo cliente 124 y el visualizador de dispositivo lector 127 puede comprender, por ejemplo, uno o más dispositivos tales como visualizadores de pantalla de cristal líquido (LCD), visualizadores de panel plano basado en plasma de gas, visualizadores de diodo orgánico emisor de luz (OLED), visualizadores de tinta electroforética (tinta E), proyectores de LCD u otros tipos de dispositivos de visualización, *etc.*

El dispositivo cliente 106 puede configurarse para ejecutar diversas aplicaciones tales como una aplicación cliente 130 y/u otras aplicaciones. La aplicación cliente 130 puede ejecutarse en el dispositivo cliente 106, por ejemplo, para realizar un proceso de ingestión, por el que una serie de interfaces de usuario 131a se representan en el visualizador de dispositivo cliente 124 para avisar al usuario para entrada de usuario. En un ejemplo, se proporcionan una o más preguntas al usuario para obtener información personal, información médica u otra información adecuada. La una o más preguntas pueden obtenerse del entorno informático 103 o preprogramarse en la aplicación cliente 130.

La aplicación cliente 130 puede encriptar la entrada de usuario y generar un identificador legible por máquina 133 con la entrada de usuario encriptada. Como puede apreciarse, el dispositivo lector 109 usa una aplicación de lector 136 para interpretar el identificador legible por máquina 133 y acceder a la entrada de usuario encriptada. Usando una o más claves criptográficas 121, la aplicación de lector 136 puede desencriptar la entrada de usuario encriptada para almacenamiento local en el dispositivo lector 109 o para almacenamiento remoto.

En algunas realizaciones, la aplicación cliente 130 y la aplicación de lector 136 pueden comprender, por ejemplo, un navegador, una aplicación especializada, *etc.,* y la interfaz de usuario 131a generada por la aplicación cliente 130 o la interfaz de usuario 131b generada por la aplicación de lector 136 puede comprender una página de red, una pantalla de aplicación, *etc.* El dispositivo cliente 106 puede configurarse para ejecutar aplicaciones más allá de la aplicación cliente 130 tales como, por ejemplo, aplicaciones de correo electrónico, aplicaciones de redes sociales, procesadores de texto, hojas de cálculo y/u otras aplicaciones.

El dispositivo lector 109 puede incluir un dispositivo de formación de imágenes frontal 139 o un dispositivo de formación de imágenes trasero (no mostrados), tal como una cámara u otro dispositivo capaz de interpretar el identificador legible por máquina 133. La aplicación de lector 136 puede ejecutarse en el dispositivo lector 109 para capturar una o más imágenes del identificador legible por máquina 133 generadas por la aplicación cliente 130. De manera similar, el dispositivo cliente 106 puede comprender uno o más dispositivos de formación de imágenes, tal

como una cámara frontal o trasera. En diversas realizaciones, la aplicación de lector 136 se ejecuta adicionalmente para desencriptar la entrada de usuario encriptada obtenida desde el identificador legible por máquina 133 y presenta la información de salud en el visualizador de dispositivo lector 127.

La aplicación de lector 136 puede configurarse para mantener versiones de datos proporcionados por el usuario y generar una interfaz adecuada que facilita navegar entre tipos de datos particulares o diferentes versiones. Mientras la aplicación cliente 130 puede configurarse para abstenerse de transmitir información médica u otros tipos de información a través de la red 112, en algunas realizaciones, la aplicación de lector 136 puede comunicar datos a un servicio remoto o basado en la nube, tal como un sistema electrónico de historia clínica de conformidad con HIPAA. Mientras la aplicación cliente 130 puede no enviar información de salud u otros tipos de información a través de la red 112, el entorno informático 103 puede respaldar o almacenar versiones del identificador legible por máquina 133 en el almacenamiento de datos 115. Cuando un usuario actualiza o sustituye su dispositivo cliente 106, el identificador legible por máquina 133 puede usarse para rellenar datos en el nuevo dispositivo cliente 106.

Los datos almacenados en el almacenamiento de datos 115 pueden incluir datos de dispositivo 142 así como otros datos como puede apreciarse. Los datos de dispositivo 142 pueden incluir información asociada con uno o más dispositivos cliente 106 y dispositivos lectores 109. En un ejemplo, cada dispositivo lector 109 puede asociarse con una clave criptográfica única 121 en la que la aplicación de gestión de clave 118 envía la clave criptográfica 121 a la aplicación cliente 130. La aplicación cliente 130 puede generar, a continuación, un identificador legible por máquina 133 que incluye datos de entrada de usuario encriptados con la clave criptográfica 121 para el dispositivo lector 109. Como el dispositivo lector 109 también mantiene una copia de su clave criptográfica 121, es capaz de desencriptar e interpretar la entrada de usuario datos.

En otro ejemplo, cada dispositivo cliente 106 puede asociarse con una o más claves criptográficas 121 en el que la aplicación de gestión de clave 118 envía las claves criptográficas 121 a los dispositivos lectores 109 por la instrucción de un usuario de la aplicación cliente 130. La aplicación cliente 130 puede generar un identificador legible por máquina 133 que incluye datos de entrada de usuario encriptados con la una o más claves criptográficas 121. La aplicación de gestión de clave 118, por la instrucción del usuario de la aplicación cliente 130 por ejemplo, puede enviar una clave criptográfica 121 al dispositivo lector 109 de modo que puede desencriptar e interpretar la entrada de usuario datos.

Los datos de dispositivo 142 pueden incluir identificadores de dispositivo 145 que identifican inequívocamente un dispositivo cliente 106 o un dispositivo lector 109. Los datos de dispositivo 142 pueden incluir adicionalmente perfiles de dispositivo 148 que, a su vez, pueden incluir niveles de acceso 152. En algunas realizaciones, un usuario de la aplicación cliente 130 puede asociar ciertos dispositivos lectores 109 con niveles de acceso 152 particulares. En un ejemplo, una persona puede asociar un primer dispositivo lector 109 para su médico de cabecera con un primer nivel de acceso y un segundo dispositivo lector 109 para su dentista con un segundo nivel de acceso. Para este fin, el usuario de la aplicación cliente 130 puede designar qué datos son accesibles por qué dispositivo lector 109 basándose en el nivel de acceso. Como se describirá, la entrada de usuario puede segmentarse o dividirse por información disponible para cada dispositivo lector 109. Para este fin, la aplicación de lector 136 puede proporcionar niveles diferenciados de acceso a la información especificada por el usuario o predeterminada por el entorno informático 103.

Las claves criptográficas 121 pueden incluir una cadena numérica, binaria o alfanumérica usada para encriptar datos. En diversas realizaciones, las claves criptográficas 121 pueden comprender claves criptográficas simétricas 121, claves criptográficas asimétricas 121 o una combinación de las mismas.

Con referencia a la Figura 2, se muestra otro ejemplo del entorno en red 100 según diversas realizaciones. En algunas circunstancias, los datos de entrada proporcionados por el usuario de la aplicación cliente 130 pueden manipularse en el dispositivo lector 109 u otro dispositivo con acceso a la información desencriptada. Por ejemplo, un doctor puede alterar datos proporcionados por el usuario para incluir presión sanguínea actual, peso u otra información. El usuario puede desear almacenar esta información en su dispositivo cliente 106 para mantener un historial médico más completo y preciso.

Para este fin, en algunas realizaciones, la aplicación de lector 136 puede utilizar su clave criptográfica 121 (u otra clave criptográfica 121 disponible para el dispositivo cliente 106) para proporcionar al dispositivo cliente 106 datos actualizados, modificados, complementados o manipulados de otra manera. La aplicación cliente 130 puede facilitar la captura de una o más imágenes del identificador legible por máquina 133 generadas en el dispositivo lector 109 y representadas en el visualizador de dispositivo lector 127.

En diversas realizaciones, los datos subyacentes del identificador legible por máquina 133 generados por la aplicación de lector 136 se encriptan usando una clave criptográfica 121 disponible únicamente para el dispositivo cliente 106 y el dispositivo lector 109. La aplicación cliente 130 puede desencriptar los datos subyacentes y almacenar los datos localmente en el dispositivo cliente 106. Si el usuario realiza partes de proceso de ingestión, los datos actualizados pueden proporcionarse en campos rellenados automáticamente en la interfaz de usuario 131. Escaneando el identificador legible por máquina 133 y teniendo las claves criptográficas 121 adecuadas para

acceder a los datos subyacentes, la aplicación de lector 136 puede actualizar localmente datos almacenados y puede interactuar con otras aplicaciones, tales como aplicaciones de planificación, aplicaciones de gestión de citas, aplicaciones de reposición de medicación o aplicaciones de EHR, para actualizar información asociada con la misma.

Haciendo referencia a continuación a la Figura 3, se muestra un ejemplo de una estructura de datos 300 que comprende datos usados para generar una imagen del identificador legible por máquina 133a... 133c. La estructura de datos 300 puede incluir, por ejemplo, un nivel de corrección de errores 303, un indicador de recuento de caracteres 306, un indicador de modo 309, una carga útil 312, una corrección de errores 315 y/u otros datos como puede apreciarse.

Códigos de matriz, también denominados como códigos de respuesta rápida (QR), emplean tradicionalmente corrección de errores de Reed-Solomon que se usa para generar palabras clave de corrección de errores (bytes) basándose en los datos codificados. Una aplicación de lector 136a.... 136b puede usar este nivel de corrección de errores 303 para determinar si los datos se leyeron incorrectamente y, si es así, corregir los errores en los datos usando las palabras clave de corrección de errores. Para códigos de matriz, existen cuatro niveles de niveles de corrección de errores 303 designados como L, M, Q y H con capacidades de corrección de errores de 7 %, 15 %, 25 % y 30 %, respectivamente.

Los códigos de matriz tienen diferentes tamaños, y un código de matriz de un tamaño particular se denomina como una versión. Existen cuarenta versiones disponibles, aunque son posibles versiones adicionales y se incluyen dentro del alcance de la divulgación. Por ejemplo, la versión 1 es la versión más pequeña de un código de matriz, y tiene un tamaño de 21 píxeles por 21 píxeles. Cada versión es 4 píxeles mayor que la versión anterior. La versión 4 es la versión más grande, y es de 177 píxeles por 177 píxeles. La versión más grande tiene la mayor capacidad de caracteres, como se muestra en la tabla de la Figura 4.

La carga útil 312 puede codificarse según diferentes modos como se establece por el indicador de modo 309. El indicador de modo 309 puede comprender una cadena de cuatro bits, como se muestra en la Figura 5. Los datos codificados pueden comenzar con el indicador de modo apropiado que indica el modo usado para los bits posteriores. La versión más grande de código de matriz tiene la mayor capacidad de caracteres, como se muestra en la tabla de la Figura 4. El indicador de recuento de caracteres 306 incluye el número de caracteres que se están codificando.

Para generar el identificador legible por máquina 133, la aplicación cliente 130 (o la aplicación de lector 136) puede acceder a la entrada de usuario recibida durante el proceso de ingestión y encriptar los datos usando una clave criptográfica 121. En realizaciones en las que la clave criptográfica 121 es asimétrica, puede emplearse RSA u otro algoritmo de encriptación adecuado. En realizaciones en las que la clave criptográfica 121 es simétrica, puede emplearse la Norma de Encriptación Avanzada (AES) u otro algoritmo de encriptación adecuado. La entrada de usuario encriptada puede codificarse según el indicador de modo 309. Por ejemplo, suponiendo que la entrada de usuario encriptada es una cadena de caracteres alfanuméricos, el indicador de modo 309 puede establecerse a 0010. La codificación alfanumérica puede incluir romper una cadena en pares y crear un número binario para cada par.

Los datos destinados para un primer dispositivo lector 109a pueden encriptarse usando una clave criptográfica 121 accesible por el primer dispositivo lector 109a (clave criptográfica $121_A$ mostrada en la Figura 3) y codificados como carga $útil_A$. De manera similar, los datos destinados para un segundo dispositivo lector 109b pueden encriptarse usando una clave criptográfica 121 accesible por el segundo dispositivo lector 109b (clave criptográfica $121_B$ mostrada en la Figura 3) y codificados como carga $útil_B$. Cuando se escanea por un dispositivo lector 109, únicamente una porción de la carga $útil_{Total}$ puede interpretarse por el dispositivo lector 109.

Haciendo referencia a continuación a la Figura 6, se muestra un diagrama de flujo que ilustra la transformación de datos de entrada en un código de matriz u otro identificador legible por máquina 133. Comenzando con la etapa 603, se accede a una entrada de usuario. La entrada de usuario puede incluir, por ejemplo, información de salud, información de contacto de emergencia u otro tipo de información obtenida durante el proceso de ingestión o desde una interfaz de usuario 131 presentada por la aplicación cliente 130. En el ejemplo de la Figura 6, una cadena de entrada de usuario incluye "Hola mundo" para fines explicativos.

En la etapa 606, una clave criptográfica 121 se identifica basándose en un dispositivo lector 109 para el que se conciben los datos. Por ejemplo, un usuario puede especificar una porción particular de su historial médico destinada para su médico de cabecera. Puede identificarse una clave criptográfica 121 para uno o más dispositivos lectores 109 para el médico de cabecera. En la etapa 609, la entrada de usuario se encripta usando la clave criptográfica 121 identificada en 606. Usando la encriptación de AES y la clave de "ejemploclaveencriptación", una cadena de datos encriptados incluye "BBd2iHwO/gy+xnFUg6HeAA==".

A continuación, en la etapa 612, los datos encriptados se codifican usando modo alfanumérico u otro modo adecuado, tal como numérico, byte, Kanji o ECI. Para los dos primeros caracteres "BB" en los datos encriptados, se

genera un número binario usando codificación alfanumérica para obtener "111111010". Esto puede continuar hasta que todos los datos encriptados se codifican usando un modo adecuado. Finalmente, en la etapa 615, la imagen del código de matriz se genera usando los datos codificados como la carga útil según la norma de código de matriz.

En diversas realizaciones, puede emplearse el algoritmo de encriptación AES-256 para encriptar los datos subyacentes. Puede emplearse un vector de inicialización (IV) o variable de inicio (SV) para su uso por un modo que aleatoriza la encriptación y produce criptogramas distintos, incluso si el mismo texto plano se encripta múltiples veces. (AES CBC Pkcs7). Algunos modos, tales como Libro de Códigos Electrónico (ECB) y Concatenación de Bloques de Cifrado (CBC), pueden requerir que el bloque final se rellene antes de la encriptación, por tanto, puede emplearse un relleno adecuado.

En una realización en la que se emplea AES-256, una clave criptográfica 121 puede incluir 256 bits (32 bytes) con un IV de 128 bits (16 bytes). El IV puede generarse aleatoriamente en cada encriptación realizada por la aplicación cliente 130 o la aplicación de lector 136 para proporcionar un resultado de encriptación distinto (diferentes de encriptaciones anteriores), incluso si los datos a encriptar no han cambiado. El IV generado puede almacenarse con los datos encriptados localmente en el dispositivo cliente 106 o el dispositivo lector 109 permitiendo una desencriptación futura, como se analiza en este documento.

En algunas realizaciones, los datos encriptados se almacenan localmente en el dispositivo cliente 106 o el dispositivo lector 109 en asociación con una contraseña, datos biométricos o un código PIN. Adicionalmente, cada usuario, o entidad para la que se proporcionan datos (por ejemplo, paciente, familiar, mascota) puede tener su propia clave criptográfica 121 (es decir, clave de encriptación). Como resultado, cualquier dato encriptado en un dispositivo específico puede desencriptarse únicamente en ese dispositivo cuando se proporciona la contraseña, datos biométricos o código PIN adecuado.

Ya que el algoritmo de encriptación AES requiere una clave criptográfica 121 y un IV para encriptar o desencriptar datos, el IV puede almacenarse en asociación con los datos encriptados para desencriptarse satisfactoriamente en un momento futuro. En algunas realizaciones, el servicio de gestión de clave 115 gestiona el almacenamiento y transmisión del IV a los dispositivos cliente 106 o dispositivos lectores 109 junto con la clave criptográfica 121. La clave de IV puede comprender 16 bytes u otra longitud adecuada. En algunas realizaciones, la clave de IV puede dividirse y almacenarse en ubicaciones predefinidas junto con la clave criptográfica 121. Por ejemplo, un primer número de bytes de la clave de IV puede situarse en una primera ubicación en la clave criptográfica 121 mientras un segundo número de bytes de la clave de IV puede situarse en una segunda ubicación en la clave criptográfica 121, y así sucesivamente. La clave de IV puede eliminarse de la clave criptográfica 121 antes de que se use la clave criptográfica 121. Esta característica añade un nivel de seguridad adicional en los datos encriptados. Por ejemplo, incluso si se intercepta la clave criptográfica 121, se adivina satisfactoriamente mediante fuerza bruta, etc., sin conocer como recuperar el IV de los datos, será difícil, si no imposible, desencriptar los datos encriptados.

Las Figuras 7A-7N muestran diversos ejemplos de interfaces de usuario 131 de la aplicación cliente 130 usada para realizar un proceso de ingestión avisando al usuario con diversos tipos de entrada de usuario. Como puede apreciarse, antes de realizar el proceso de ingestión, puede requerirse al usuario que proporcione un nombre de usuario, una contraseña, información biométrica u otra información para autenticar apropiadamente al usuario del dispositivo cliente 106. En la Figura 7A, se muestra una pantalla de inicio ilustrativa para la aplicación cliente 130 en la que el usuario puede introducir información primaria para un individuo. Esta puede no incluir información médica, sino información para propósitos de identificación. Esta puede usarse para identificar un nombre del individuo (por ejemplo, el propietario, dependiente, mascota u otro individuo).

Posteriormente, la aplicación cliente 130 puede avisar al usuario que introduzca información básica, tal como fecha de nacimiento, información de contacto de emergencia, información de contacto de médico de atención primaria u otra información básica. También la interfaz de usuario 131 puede permitir que un usuario cambie el individuo para el que se proporciona información. Por ejemplo, el usuario puede cambiar el individuo desde sí mismo a otro individuo, tal como un hijo, dependiente, mascota, etc. Estos perfiles secundarios también tendrán campos de datos para colocar información para médicos de atención primaria, información de contacto de emergencia, historial médico, etc.

La Figura 7B muestra una realización de una interfaz de usuario 131 de documentación y de conformidad con la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA). A partir de esta interfaz de usuario 131, se muestra información que pertenece a diversas regulaciones, tal como HIPPA, seguida de una explicación adecuada para obtener consentimiento requerido. En diversas realizaciones, puede generarse un enlace u otro componente de interfaz de usuario que provoca que otra aplicación, tal como una aplicación de navegador, muestre información para la que necesitan una explicación adicional en cuanto a los detalles de cumplimiento. Tras la revisión, puede hacerse un aviso para una firma electrónica y una fecha o indicación de tiempo para verificar que el usuario ha revisado el material y obtener el consentimiento requerido.

Pasando ahora a la Figura 7C, una interfaz de usuario 131 ilustra una realización de la pantalla dedicada para obtener información médica pasada para un individuo. La interfaz de usuario 131 de la Figura 7C habilita que un

usuario proporcione diagnósticos médicos que se han dado en el pasado por un profesional médico. En diversas realizaciones, texto inteligente, autorrelleno, sugerencias desplegables y/u otros componentes similares pueden incluirse para facilitar una ortografía correcta de las dolencias y/o enfermedades más comunes. La aplicación cliente 130 también puede obtener datos relacionados con la fecha en la que se proporcionó este diagnóstico. Estos pueden a continuación colocarse en orden numérico basándose en las fechas. En el caso en que un diagnóstico no esté listado, puede estar disponible una opción de texto libre. Puede crearse una casilla de texto adicional para información adicional que puede ser importante.

La Figura 7D muestra una interfaz de usuario 131 en la que puede obtenerse información quirúrgica pasada avisando al usuario para que proporcione todas las experiencias quirúrgicas anteriores. Como se ha indicado anteriormente, en diversas realizaciones, pueden incluirse texto inteligente, autorrelleno, sugerencias desplegables y/u otros componentes similares para facilitar una ortografía correcta de las operaciones o procedimientos médicos más comunes. Si se conoce, también puede obtenerse la fecha e institución de estos procedimientos quirúrgicos. Los procedimientos quirúrgicos se colocarán a continuación en orden temporal con campos de datos asociados para fecha e institución en la que se realizó el procedimiento. En el caso de que un procedimiento no esté listado, habrá disponible una opción para texto libre.

Haciendo referencia a continuación a la Figura 7E, se muestra una interfaz de usuario 131 que ilustra una realización de una pantalla dedicada para obtener medicaciones actuales y pasadas que habilita que el usuario proporcione medicaciones actuales y anteriores. En diversas realizaciones, texto inteligente, autorrelleno, sugerencias desplegables y/u otros componentes similares pueden incluirse para facilitar una ortografía correcta de las medicaciones más comunes. Pueden incluirse la fecha en la que se inició la medicación proporcionada, la razón para la medicación y la dosis y frecuencia de administración. En el caso de que esta sea una medicación antigua que el usuario ya no está tomando, se incluirá un campo para fecha en la que la se detuvo la medicación con una razón de porqué se paró de tomar. En el caso de que una medicación no esté listado, habrá disponible una opción para texto libre.

La Figura 7F muestra una interfaz de usuario 131 en la que un usuario puede proporcionar alergias actuales y pasadas, medicaciones, desencadenadores ambientales, animales y otra información relevante. En diversas realizaciones, texto inteligente, autorrelleno, sugerencias desplegables y/u otros componentes similares pueden incluirse para facilitar una ortografía correcta de las medicaciones y alérgenos más comunes. También se incluirá el tipo de reacción al alérgeno. Estos también se colocarán en orden numérico con un campo asociado para el tipo de reacción a cada alérgeno.

En el ejemplo no limitante de la Figura 7G, se muestra una interfaz de usuario 131 que habilita que un usuario proporcione información asociada con el historial médico de su familia. En algunas realizaciones, puede presentarse al usuario condiciones médicas comunes específicas para advertir si es aplicable al historial médico familiar. Pueden usarse campos de datos adecuados para enfermedades no comunes. Además, texto inteligente, autorrelleno, sugerencias desplegables y/u otros componentes similares pueden incluirse para facilitar una ortografía correcta de dolencias o enfermedades comunes. El usuario también puede caracterizar qué miembro familiar poseía este diagnóstico con su edad y año de "defunción", si es aplicable.

La Figura 7H ilustra una realización de una interfaz de usuario 131 dedicada a la obtención de un historial social de un usuario. Por ejemplo, puede presentarse a un usuario un formulario para proporcionar información asociada con el historial social de un individuo. En algunas realizaciones, el formulario incluye campos de datos que cubren historial de tabaco, consumo de alcohol, viajes al extranjero, nivel de estudios, etc. Esto también puede incluir información pediátrica específica tal como compañeros residentes en el hogar, armas de fuego en la casa, animales en la casa, exposición a plomo y tuberculosis, etc., basándose en la edad calculada a partir de la fecha de nacimiento proporcionada anteriormente.

Haciendo referencia a continuación a la Figura 7I, una interfaz de usuario 131 ilustra una realización que obtiene inmunizaciones de un usuario. Puede emplearse texto inteligente para ayudar al usuario a escribir correctamente las inmunizaciones. Puede proporcionarse campos de texto abierto para inmunizaciones que no se dan comúnmente ya que pueden necesitarse para viajes al extranjero. En algunas realizaciones, la fecha que se proporcionó la inmunización puede ser un campo requerido. Esta información puede situarse en orden cronológico basándose en la fecha de inmunización.

La Figura 7J muestra una realización de una interfaz de usuario 131 que habilita que un usuario proporcione notas diversas que pueden retenerse localmente únicamente para su acceso por el usuario o pueden incluirse en el identificador legible por máquina 133. Por ejemplo, las notas pueden incluir un recordatorio con respecto a una cita de atención sanitaria específica. En diversas realizaciones, esto puede limitarse a 100 caracteres u otra cantidad adecuada ya que esta no es una lista de síntomas, sino solo un recordatorio de una visita específica. Como con cualquier otra sección, la página de notas puede dejarse en blanco si no hay necesidad de actualizar esta información. En algunas realizaciones, los datos proporcionados en el campo de notas pueden excluirse de los datos del identificador legible por máquina 133.

La Figura 7K muestra otro dibujo del dispositivo cliente 106 que genera una interfaz de usuario 131 en el visualizador de dispositivo cliente 124. En el ejemplo no limitante de la Figura 7K, se muestra una realización en la que se proporciona a un usuario información anteriormente proporcionada por el usuario. Como puede apreciarse, en realizaciones en las que se obtiene información de salud, puede adquirirse idealmente información que pertenece a uno o más de los once sistemas de órganos. La interfaz de usuario 131 puede facilitar imprimir o transferir paquetes de información a un médico u otra persona interesada en un formato predefinido por el usuario, un administrador o un formato especificado por un proveedor de atención sanitaria. Esto proporciona la capacidad de correlacionar esta información en un formato que es preferido por médicos y legible tanto para el propietario como el médico. En otros ejemplos, la interfaz de usuario 131 puede recibir información asociada con la farmacia de un paciente, seguro u otros temas relacionados. El proceso de ingestión puede incluir una revisión de sistemas corporales así como exploraciones de salud.

Además, la aplicación cliente 130 puede organizar información proporcionada durante el proceso de ingestión en un formato predefinido. En un ejemplo, la información puede clasificarse cronológicamente y por tema, tal como alergias o medicaciones. Para realizaciones en las que la información son datos médicos, el formato cronológico, común a proveedores de asistencia sanitaria, proporciona una forma de presentar de forma eficiente los datos obtenidos usando la aplicación cliente 130. Proporcionará toda la información de salud designada como requerida por el proveedor de asistencia sanitaria. Debido a que la información proporcionada puede ser completa y precisa, puede ayudar en la limitación de errores médicos mediante la correcta identificación de medicaciones y alergias, así como proporcionando la totalidad del historial médico que puede resultar necesario para el médico o proveedor.

Los datos pueden formatearse y/o comprimirse antes de la encriptación por la aplicación cliente 130, o la aplicación de lector 136 puede formatear los datos cuando se desencriptan y/o descomprimen. Por consiguiente, cualquiera de la aplicación cliente 130 o la aplicación de lector 136 puede formatear los datos en un formato predefinido, tal como el formato de Arquitectura de Documentos Clínicos (CDA) que incluye una norma de marcado flexible desarrollado por Health Level 7 International. El formato de CDA incluye una estructura predefinida de ciertas historias clínicas, tales como descarga de resúmenes y notas de progreso para intercambiar información entre pacientes y profesionales médicos. El formato de CDA permite la inclusión de texto, imágenes y otros tipos de multimedia, tales como audio o video. En otros ejemplos, el formato puede especificarse por el proveedor de atención sanitaria a través de la aplicación de lector 136.

En diversas realizaciones, la aplicación cliente 130 puede exportar un resumen de la información en un formato de Microsoft Word®, PDF® u otro formato adecuado para que un usuario lo imprima en la consulta de un proveedor de atención sanitaria o antes de la visita. En algunas realizaciones, el identificador legible por máquina 133 puede colocarse en la esquina del documento generado o en otra ubicación adecuada. Usando un dispositivo lector 109, el proveedor de asistencia sanitaria puede escanear el identificador legible por máquina 133 desde el visualizador de dispositivo cliente 124 o un documento para importar esta información en un expediente o historia clínica electrónica (EHR), dependiendo de las costumbres de la práctica particular. Como puede apreciarse, un dispositivo lector 109 para el proveedor de asistencia sanitaria puede ser capaz de desencriptar información proporcionada por el identificador legible por máquina 133, ya que la aplicación cliente 130 puede configurarse para encriptar la información de salud antes de la generación del identificador legible por máquina 133. Como resultado, un usuario de la aplicación cliente 130 puede evitar el largo proceso de rellenar formularios de admisión médicos, por ejemplo, mientras está sentado en una consulta. Ya que la información proporcionada por el usuario puede actualizarse por el profesional médico, puede ayudar en la limitación de errores médicos mediante la correcta identificación de medicaciones y alergias, así como proporcionando la totalidad del historial médico que puede resultar necesario para el médico.

La aplicación cliente 130 puede incluir una aplicación móvil o una aplicación basada en web accedida a través de una aplicación de navegador. Los individuos que usan la aplicación basada en web pueden ser capaces de convertir la información de resumen en un formato de Word® o PDF® para que el propietario la imprima antes de la visita y la información puede borrarse tras terminar una sesión. En la esquina de la impresión, puede mostrarse el identificador legible por máquina 133 asociado.

Basándose en la discreción y capacidades del proveedor de asistencia sanitaria, otra realización especifica que la aplicación cliente 130 genera un correo electrónico con un adjunto de la información y/o el identificador legible por máquina 133 a enviar por correo electrónico y compartir electrónicamente con el proveedor de asistencia sanitaria, personal de consulta o sistema sanitario. Esto puede completarse por el propietario o bien desde casa antes de la visita o mientras está en la sala de espera del proveedor de asistencia sanitaria. El formato de la información será el que se prefiera por el proveedor de asistencia sanitaria. A partir de este punto, puede imprimirse para añadirse al expediente de papel del paciente, escanearse o introducirse manualmente en la historia clínica electrónica. Finalmente, puede enlazarse electrónicamente a un EHR o sistema electrónico de historia clínica (EMR) propietario. Antes de compartir esta información electrónicamente, puede requerirse que el propietario revise de nuevo las regulaciones de la HIPAA y para una firma electrónica y fecha/indicación de tiempo para la revisión de esta información.

Pasando ahora a la Figura 7L, puede mostrarse un identificador legible por máquina 133 que tiene la entrada de

usuario proporcionada durante el proceso de ingestión. Sujetando la imagen encriptada hasta una lente o cámara de un dispositivo lector 109, la información de salud encriptada puede transferirse para interpretación por el dispositivo lector 109. En algunas realizaciones, un dependiente puede transferir su información al dispositivo cliente 106 de un padre, o viceversa, capturando una imagen del identificador legible por máquina 133. La aplicación de gestión de clave 118 facilita la transferencia de las claves criptográficas 121 adecuadas cuando se obtiene un consentimiento requerido.

Con referencia a la Figura 7M, un usuario de la aplicación cliente 130 puede especificar la clave criptográfica 121 y un destinatario de los datos, tal como un propietario de un dispositivo lector 109 o un dispositivo cliente 106 diferente. En otras realizaciones, la clave criptográfica 121 puede generarse pseudoaleatoriamente por la aplicación cliente 130 o la aplicación de gestión de clave 118. Si se genera por la aplicación cliente 130, la clave criptográfica 121 se transmite a la aplicación de gestión de clave 118 que, a su vez, comunica la clave criptográfica 121 a un dispositivo lector 109 u otro dispositivo cliente 106 según se ordene por un usuario de la aplicación cliente 130. Por ejemplo, el usuario del dispositivo cliente 106 puede tener la clave criptográfica 121 transmitida a uno o más dispositivos lectores 109 como asociada con el proveedor "Atlanta Health". En otras realizaciones, una clave criptográfica predefinida 121 se usa basándose en la selección del proveedor. Por ejemplo, la aplicación de gestión de clave 118 puede almacenar una o más claves criptográficas 121 para el proveedor "Atlanta Health". Cuando se selecciona "Atlanta Health", la aplicación cliente 130 puede usar la una o más claves criptográficas 121 almacenadas en asociación con el proveedor "Atlanta Health" para encriptar información para su uso en un identificador legible por máquina 133.

En realizaciones adicionales, la clave de criptografía 121 puede establecerse como una fecha de nacimiento, número de la seguridad social u otra constante que puede no estar disponible de forma generalizada o pública. Puede permitirse a cualquier proveedor de asistencia sanitaria que obtiene software necesario para leer y transferir la información representada en la imagen de QR encriptada, a continuación, que extraiga instantáneamente la entrada de usuario electrónica e inalámbricamente. En algunas realizaciones, puede emplearse una capa de seguridad adicional en la que puede requerirse que el destinatario de la información entre en otro identificador específico para el usuario originador, tal como una fecha de nacimiento o número de la seguridad social, antes de que la información se desencripte.

El proceso de extracción de la información puede lograrse sujetando el identificador legible por máquina 133 hacia una lente de cámara del dispositivo lector 109 u otro dispositivo cliente 106 en posesión por un proveedor de atención sanitaria u otra persona interesada. Como puede apreciarse, esto puede realizarse por personal en una ventanilla y en un minuto o menos. La información obtenida puede usarse a continuación por la aplicación de lector 136 u otras aplicaciones en el dispositivo lector 109 para añadir al expediente de papel de un paciente o un sistema electrónico de historia clínica. Adicionalmente, la aplicación de lector 136 puede configurarse para rellenar automáticamente campos en sistemas EMR de terceros.

Haciendo referencia a continuación a la Figura 7N, la aplicación cliente 130 puede facilitar enviar mensajes encriptados desde un dispositivo cliente 106 a otro. En un ejemplo, la aplicación cliente 130 permite que un paciente se comunique directamente con su proveedor sanitario. La aplicación cliente 130 puede encriptar un mensaje generado por un usuario del dispositivo cliente 106 y enviar el mensaje encriptado al servicio de mensajería directa 122 a través de la red 112. El servicio de mensajería directa 122 puede transmitir, a continuación, el mensaje encriptado a un dispositivo cliente receptor 106. En otras realizaciones, pueden pasarse mensajes entre dispositivos cliente 106 usando un identificador legible por máquina 133. La aplicación cliente 130 puede adicionalmente facilitar la transmisión del identificador legible por máquina 133 a través del servicio de mensajería directa 122.

Pasando ahora a la Figura 8, se muestra pseudocódigo 800 que puede implementarse en la configuración de la aplicación cliente 130, la aplicación de lector 136 u otra aplicación apropiada para generar un código de matriz u otro tipo de identificador legible por máquina 133. Por ejemplo, una función en la Línea 01 del pseudocódigo puede llamarse programáticamente para generar un código de matriz. La Línea 02 recibe la entrada de usuario a incluirse en el identificador legible por máquina 133, tal como una entrada de usuario proporcionada en el proceso de ingestión realizado presentando la interfaz de usuarios 131 de las Figuras 7A-7K. Ya que la entrada de usuario se almacena localmente en el dispositivo cliente 106, puede requerirse apropiadamente.

En la Línea 03, se obtiene una clave criptográfica 121 usando una llamada de función apropiada. En la realización de la Figura 8, la clave criptográfica 121 se obtiene basándose en un identificador proporcionado para un dispositivo lector 109 particular. Por ejemplo, un usuario de la aplicación cliente 130 puede especificar del destinatario previsto de los datos. En otras realizaciones, el usuario puede especificar su propia clave criptográfica 121. En realizaciones adicionales, la clave criptográfica 121 puede generase pseudoaleatoriamente o determinarse usando una fecha de nacimiento, número de la seguridad social u otra información proporcionada por el usuario.

En la Línea 04, se establece un indicador de modo 309. En el ejemplo de la Figura 8, el indicador de modo se establece a "0010" que indica modo alfanumérico. En la Línea 05, se determina el recuento de caracteres de los datos de entrada. En la Línea 06, se hace una llamada de función a una función apropiada que encripta la entrada de usuario usando la clave criptográfica 121, devolviendo una cadena encriptada y otro tipo de variable adecuada.

En la Línea 07, se determina un código de error de Reed-Solomon usando una llamada de función apropiada. En las Líneas 08-09, los datos pueden formatearse. En la Línea 10, los datos formateados se proporcionan como una variable de una llamada de función programática para generar el identificador legible por máquina 133 en una imagen u otro formato apropiado.

Pasando ahora a la Figura 9, se muestra otro ejemplo de la aplicación cliente 130 que importa datos desde una fuente externa. Como se ha indicado anteriormente, en algunas circunstancias, datos de entrada proporcionados por un usuario de la aplicación cliente 130 pueden manipularse en el dispositivo lector 109 u otro dispositivo con acceso a la información desencriptada. Por ejemplo, un doctor puede actualizar o alterar los datos para incluir una lectura presión sanguínea, medición de peso, medición de nivel de glucosa u otra información actualizada. El usuario puede desear almacenar esta información actualizada en su dispositivo cliente 106 para mantener un historial médico más completo y preciso. En algunas realizaciones, la aplicación de lector 136 puede generar un documento 900 capaz de imprimirse para su inserción en un archivo médico físico.

La aplicación de lector 136 puede utilizar su clave criptográfica 121 para generar el documento 900 que tiene el identificador legible por máquina 133a...133b. La aplicación de gestión de clave 118 puede proporcionar al dispositivo cliente 106 una clave criptográfica 121 adecuada basándose en el dispositivo lector 109, u otro dispositivo, que generó el identificador legible por máquina 133. La aplicación cliente 130 puede facilitar la captura de una o más imágenes del identificador legible por máquina 133 colocadas en el documento 900. Una vez que se obtiene una imagen del identificador legible por máquina 133 en el dispositivo cliente 106 y desencripta, el dispositivo cliente 106 puede actualizar localmente información almacenada y/o rellenar automáticamente campos en una interfaz de usuario 131 para revisión por el usuario.

En diversas realizaciones, los datos subyacentes del identificador legible por máquina 133 generados por la aplicación de lector 136 se encriptan usando una clave criptográfica 121 disponible únicamente para el dispositivo cliente 106 y el dispositivo lector 109. La aplicación cliente 130 puede desencriptar los datos subyacentes y almacenar los datos localmente en el dispositivo cliente 106. Si el usuario realiza partes de proceso de ingestión, los datos actualizados pueden proporcionarse en campos rellenados automáticamente en la interfaz de usuario 131.

Se construyen múltiples mecanismos de seguridad en el código e implementación de la aplicación cliente 130. Debido al alcance de la información potencialmente crítica, en diversas realizaciones, esta información se almacena localmente en el dispositivo cliente 106. Por lo tanto, la pérdida potencial de esta información a través de la "nube" se reduce o elimina. En diversas realizaciones, la aplicación cliente 130 puede integrarse con sistemas basados en la nube para la entrada y actualización remotas de información.

Además de la protección por contraseña por defecto proporcionada en teléfonos inteligentes u otros tipos de dispositivos cliente 106, puede requerirse una contraseña adicional o número de identificador personal (PIN) para acceder a características de la aplicación cliente 130. Una contraseña incorrecta proporcionada un número de veces predeterminado de forma consecutiva (por ejemplo, cinco veces) puede resultar en deshabilitar el uso de la aplicación cliente para un periodo de tiempo predefinido, tal como veinticuatro horas. Antes de compartir esta información electrónicamente, puede requerirse un identificador adicional que representa el permiso del propietario para compartir esta información.

En diversas realizaciones, puede permitirse que proveedores de asistencia sanitaria con permiso para extraer la información desde el identificador legible por máquina 133 también actualicen o aumenten la información y proporcionen de vuelta la información actualizada o aumentada al propietario en forma de otro identificador legible por máquina 133. Como resultado, la información actualizada puede conciliarse con la información ya presente en el dispositivo cliente 106. De este modo, el propietario no tendrá que introducir nueva información ya que se completará por la aplicación cliente 130. Esto también puede incluir recordatorios para futuras visitas que se incorporarán en el calendario del dispositivo móvil, recordatorios para reposiciones de medicaciones, *etc.* En otro ejemplo, la aplicación cliente 130 puede conciliar electrónicamente medicaciones con una farmacia.

La aplicación cliente 130 puede incorporarse en múltiples versiones, en la que cada versión usa un idioma diferente, tal como inglés, español, francés u otro idioma. La entrada de usuario puede traducirse desde un idioma del usuario a un idioma del destinatario por el servicio de traducción 120, si se necesita. Esto puede producirse antes de codificar los datos para su uso en el identificador legible por máquina 133 o tras decodificar la información con la aplicación de lector 136. Para esas situaciones en las que un nivel superior de comunicación o terminología médica en inglés no se conoce, esta información se usa para ayudar en una evaluación médica o de otro tipo.

En una realización, un identificador legible por máquina 133 puede codificarse en una "pantalla bloqueada" de un dispositivo cliente 106 de modo que una persona sin acceso al teléfono puede lograr acceso para la identificación, salud o información de contacto crucial sin tener que desbloquear el dispositivo cliente 106. En otras realizaciones, la información proporcionada durante un proceso de ingestión puede borrarse periódicamente en el dispositivo cliente 106 o en el dispositivo lector 109, por ejemplo, al final de una sesión de uso.

Haciendo referencia a continuación a la Figura 10, se muestra un diagrama de flujo que proporciona un ejemplo de

la operación de una porción de la aplicación cliente 130 según diversas realizaciones. Se entiende que el diagrama de flujo de la Figura 10 proporciona meramente un ejemplo de los muchos diferentes tipos de disposiciones funcionales que pueden emplearse para implementar la operación de la porción de la aplicación cliente 130 como se describe en este documento. Como una alternativa, el diagrama de flujo de la Figura 10 puede verse como que representa un ejemplo de elementos de un método implementado en el dispositivo cliente 106 según una o más realizaciones.

Comenzando con la etapa 1003, la aplicación cliente 130 se ejecuta para obtener información, tal como información de salud, desde un usuario para uno o más individuos, tal como personas dependientes, mascotas u otros animales, *etc.* Esto puede conseguirse usando la interfaz de usuarios 131 que se presenta posteriormente en un proceso de ingestión en el que un usuario itera a través de la interfaz de usuarios 131 durante una o más sesiones. A continuación, en la etapa 1006, la aplicación cliente 130 determina si una notificación de HIPAA se ha confirmado por el usuario. Si la notificación de HIPAA no se ha confirmado, la notificación de HIPAA puede representarse al usuario y el proceso puede volver a 1003 o continuar a finalizar. Si la notificación de HIPAA se ha confirmado por el usuario, el proceso puede continuar a 1009 en la que la información general, de salud u otra información proporcionada por el usuario se encripta según una o más normas de encriptación y formatos predefinidos.

En diversas realizaciones, los datos se encriptan usando una o más claves criptográficas 121. En diversas realizaciones, la clave criptográfica 121 comprende información proporcionada por el usuario, tal como a fecha de nacimiento, un apellido, un nombre, un número de la seguridad social, una combinación de los mismos u otra información potencialmente única. En 1012, la información encriptada se usa para generar un identificador legible por máquina 133, tal como un código de barras o un código de matriz. Las etapas tomadas para generar el identificador legible por máquina se describen con respecto a la Figura 6 y la Figura 8.

Haciendo referencia de nuevo a la Figura 10, en la etapa 1015, puede avisarse al usuario con una notificación adicional preguntando al usuario si el usuario desea mostrar el identificador legible por máquina 133 generado en el visualizador de dispositivo cliente 124. Finalmente, en la etapa 1018, el identificador legible por máquina puede codificarse en una interfaz de usuario 131 para representar en el visualizador de dispositivo cliente 124. En este punto, el usuario puede ser capaz de proporcionar el identificador legible por máquina 133 para su escaneo por un dispositivo lector 109 o el usuario puede imprimir un documento que contiene la información y que tiene el identificador legible por máquina 133 ubicado en el mismo.

Haciendo referencia a continuación a la Figura 11, se muestra un diagrama de flujo que proporciona otro ejemplo de la operación de una porción de la aplicación cliente 130 según diversas realizaciones. Se entiende que el diagrama de flujo de la Figura 11 proporciona meramente un ejemplo de los muchos diferentes tipos de disposiciones funcionales que pueden emplearse para implementar la operación de la porción de la aplicación cliente 130 como se describe en este documento. Como una alternativa, el diagrama de flujo de la Figura 11 puede verse como que representa un ejemplo de elementos de un método implementado en el dispositivo cliente 106 según una o más realizaciones.

Comenzando en la etapa 1103, una aplicación cliente 130 ejecutable en un dispositivo cliente 106 puede configurarse para acceder a una primera clave criptográfica 121a asociada con un primer perfil de dispositivo 148a. De manera similar, en la etapa 1106, la aplicación cliente 130 puede acceder una segunda clave criptográfica 121b asociada con un segundo perfil de dispositivo 148b recibido a través de la red 112. Como puede apreciarse, la primera clave criptográfica 121a y la segunda clave criptográfica 121b pueden enviarse al dispositivo cliente 106 mediante la aplicación de gestión de clave 118 u otro servicio similar a través de la red 112. La primera clave criptográfica 121a y la segunda clave criptográfica 121b pueden proporcionarse a la aplicación cliente 130 en respuesta a una selección de una cierta entidad u organización, tal como una consulta médica o profesional médico. En un ejemplo, la primera clave criptográfica 121a se asocia con un primer proveedor médico. El primer proveedor médico puede poseer u operar un primer dispositivo lector 109a asociado con el primer perfil de dispositivo 148a y que tiene la primera clave criptográfica 121a almacenada en el mismo. De manera similar, la segunda clave criptográfica 121b se asocia con un segundo proveedor médico, por el que el segundo proveedor médico puede poseer u operar un segundo dispositivo lector 109b asociado con el segundo perfil de dispositivo 148b y que tiene la segunda clave criptográfica 121b almacenada en el mismo.

Ya que la aplicación cliente 130 facilita la recopilación de datos de entrada desde un usuario a través de un proceso de ingestión, en la etapa 1109, los datos de entrada pueden accederse para su inclusión en un identificador legible por máquina 133. El proceso de ingestión puede incluir una serie de interfaces de usuario 131 que avisan al usuario que introduzca una diversidad de datos, tales como los mostrados en las Figuras 7A-7K. En la etapa 1112, la aplicación cliente 130 puede segmentar, dividir o formatear de otra manera los datos de entrada en al menos una primera porción de datos y una segunda porción de datos. Por ejemplo, la primera porción de datos puede ser capaz de interpretarse por un dispositivo para un médico de cabecera mientras la segunda porción de datos puede ser capaz de interpretarse por un dispositivo para un quiropráctico.

A continuación, en la etapa 1115, la aplicación cliente 130 puede encriptar la primera porción de datos usando la primera clave criptográfica 121a mientras, en la etapa 1118, la aplicación cliente 130 puede encriptar la segunda

porción de datos usando la segunda clave criptográfica 121b. La aplicación de gestión de clave 118 que opera en el entorno informático 103 puede supervisar la transmisión y recepción de claves criptográficas 121 capaces de desencriptar los datos, según se autorice por el usuario. Como alternativa, en otras realizaciones, un dispositivo lector 109 puede asociarse con una clave criptográfica predefinida 121 almacenada en el almacenamiento de datos 115 del entorno informático 103. La aplicación de gestión de clave 118 puede proporcionar a la aplicación cliente 130 con una clave criptográfica 121 para un dispositivo lector 109 particular de modo que la información se encripta para su acceso por el dispositivo lector 109 u otro dispositivo cliente 106.

En la etapa 1121, la aplicación cliente 130 puede generar un identificador legible por máquina 133 usando la primera porción de datos encriptados y la segunda porción de datos encriptados para representar en el visualizador de dispositivo cliente 124. El dispositivo lector 109 puede capturar una o más imágenes del identificador legible por máquina 133 para acceder a los datos subyacentes.

En realizaciones adicionales, un usuario de la aplicación cliente 130 puede asociar un perfil de dispositivo 148, tal como uno perteneciente a un médico de cabecera, con un alto nivel de acceso, en el que el médico de cabecera es capaz de usar su dispositivo lector 109 para acceder a toda o una cantidad sustancial de los datos de entrada proporcionados por el usuario de la aplicación cliente 130. La aplicación de gestión de clave 118 puede enviar una clave criptográfica 121 al dispositivo lector 109 para el médico de cabecera, así como al dispositivo cliente 106 para el usuario. De manera similar, la aplicación de gestión de clave 118 puede enviar una clave criptográfica 121 diferente a un dispositivo lector 109 para el quiropráctico u otro proveedor médico. La aplicación cliente 130 puede codificar datos autorizados para su recepción por el médico de cabecera usando una clave criptográfica 121 que corresponde al dispositivo lector 109 del médico de cabecera mientras codifica datos autorizados para su recepción por el quiropráctico usando una clave criptográfica 121 diferente para un dispositivo lector 109 del quiropráctico. Para este fin, usando un único identificador legible por máquina 133, se proporciona control de acceso a los datos subyacentes del identificador legible por máquina 133. Posteriormente, el proceso continúa a terminar.

En algunas realizaciones, puede definirse un primer nivel de acceso 152a asociado con la primera porción de datos. Por ejemplo, un usuario puede asociar un nivel de acceso bajo 152 requerido con su información personal mientras asocia un nivel de acceso alto 152 requerido con su historial médico. Un dispositivo lector 109 asociado con un nivel de acceso alto 152 puede acceder tanto al historial médico como la información personal mientras un dispositivo lector 109 asociado con un nivel de acceso bajo 152 puede acceder únicamente a la información personal. En un ejemplo, un entrenador de un niño puede tener un nivel de acceso bajo 152 concedido a un dispositivo cliente 106 usado para acceder a información de contacto de emergencia para un jugador, según se autoriza por el jugador o padre.

En otras palabras, el nivel de acceso 152 puede usarse para determinar a qué porciones de los datos pueden acceder los dispositivos lectores 109. El usuario también puede definir a través de la aplicación cliente 130 qué entidades, tales como consultas médicas, tienen acceso a datos asociados con diversos niveles de acceso 152. Para este fin, pueden identificarse un primer nivel de acceso 152a asociado con la primera porción de datos y un segundo nivel de acceso 152b asociado con la segunda porción de datos en los que la primera porción de datos se encriptará usando la primera clave criptográfica 121a basándose al menos en parte en el primer nivel de acceso 152a, y la segunda porción de datos se encriptará usando la segunda clave criptográfica 121b basándose al menos en parte en el segundo nivel de acceso 152b. Como puede apreciarse, el primer nivel de acceso 152a puede ser diferente que el segundo nivel de acceso 152b.

Haciendo referencia a continuación a la Figura 12, se muestra un diagrama de flujo que proporciona otro ejemplo de la operación de una porción de la aplicación cliente 130 según diversas realizaciones. Se entiende que el diagrama de flujo de la Figura 12 proporciona meramente un ejemplo de los muchos diferentes tipos de disposiciones funcionales que pueden emplearse para implementar la operación de la porción de la aplicación cliente 130 como se describe en este documento. Como una alternativa, el diagrama de flujo de la Figura 12 puede verse como que representa un ejemplo de elementos de un método implementado en el dispositivo cliente 106 según una o más realizaciones.

Comenzando con 1203, la aplicación cliente 130 puede identificar un identificador legible por máquina 133 en una imagen capturada por una cámara u otro dispositivo de formación de imágenes en comunicación con el dispositivo cliente 106. Por ejemplo, el identificador legible por máquina 133 puede ser uno generado por el dispositivo lector 109 para proporcionar datos actualizados, complementados y otros datos manipulados proporcionados inicialmente por un usuario de la aplicación cliente 130 usando un identificador legible por máquina 133 inicial generado después de completar un proceso de ingestión. Como puede apreciarse, los datos modificados por el dispositivo lector 109 pueden obtenerse a partir de un identificador legible por máquina 133 original generado en el dispositivo cliente 106. El dispositivo cliente 106 puede obtener una imagen del identificador legible por máquina 133 para actualizar sus datos almacenados localmente. La imagen puede capturarse desde el visualizador de dispositivo lector 127, como se muestra en la Figura 2, un visualizador de otro dispositivo cliente 106, o desde un documento 900, como se muestra en la Figura 9.

A continuación, en la etapa 1206, el identificador legible por máquina 133 se decodifica para identificar una cantidad

de datos encriptados. En la etapa 1209, la aplicación cliente 130 puede desencriptar la cantidad de datos encriptados usando una clave criptográfica 121 asociada con un perfil de dispositivo 148 de un dispositivo de origen desde el que se obtiene el identificador legible por máquina 133. En algunas realizaciones, una cantidad de datos leídos desde el identificador legible por máquina 133 pueden ser públicos (no encriptados) que identifica el dispositivo lector 109 del que se obtuvo el identificador legible por máquina 133 en el que cualquier dispositivo puede decodificar la cantidad de datos. La cantidad de datos puede comprender un identificador de dispositivo 145 y/o un identificador único que identifica a una persona o dispositivo cliente 106 autorizado para acceder a los datos encriptados. La aplicación cliente 130 puede comunicar el identificador de dispositivo 145 al entorno informático 103 para obtener una clave criptográfica 121 si el dispositivo cliente 106 así está autorizado.

En la etapa 1212, los datos desencriptados obtenidos a partir del identificador legible por máquina 133 pueden usarse para actualizar o complementar los datos almacenados localmente en el dispositivo cliente 106. En algunas situaciones, los datos desencriptados pueden estar en conflicto con datos proporcionados por el usuario. Por ejemplo, porciones de los datos proporcionados por el usuario al dispositivo lector 109 a través de un primer identificador legible por máquina 133 pueden haber cambiado. Como alternativa, los datos proporcionados por el usuario pueden aumentarse con lecturas tomadas por un doctor que pueden haber sido desconocidas anteriormente para el usuario.

Por consiguiente, en la etapa 1215, la aplicación cliente 130 determina si existe un conflicto entre los datos desencriptados y los datos proporcionados por el usuario, por ejemplo, a través del proceso de ingestión. Los datos pueden estar en conflicto, por ejemplo, si los datos proporcionados por el usuario usando su dispositivo cliente 106 son diferentes de los datos devueltos por el dispositivo lector 106 en cualquier respecto. Por ejemplo, usando el dispositivo lector 109, un médico o enfermera puede actualizar los datos proporcionados por el usuario para reflejar lecturas o mediciones recientes. Como alternativa, usando el dispositivo lector 109, el médico o enfermera puede aumentar los datos proporcionados por el usuario. En cualquier escenario, se identifica un conflicto entre los datos ya que ambos conjuntos de datos no son idénticos. Una función de DIFF o función similar puede emplearse para identificar porciones específicas de los datos en las que existe conflicto.

Si existe un conflicto entre los datos, el proceso continúa a la etapa 1218 para conciliar o resolver de otra manera el conflicto de datos. En algunas realizaciones, puede presentarse al usuario información que pertenece al conflicto en la que el usuario puede seleccionar si mantener los datos originales proporcionados por el usuario o actualizar los datos con los datos proporcionados desde el dispositivo lector 109. En otras realizaciones, los datos proporcionados desde el dispositivo lector 109 pueden sustituir automáticamente datos proporcionados por un usuario o añadirse automáticamente a la memoria del dispositivo cliente 106 para aumentar los datos proporcionados por el usuario durante el proceso de ingestión.

En algunos ejemplos, algunas porciones de datos pueden asociarse con niveles de acceso variables 152 que pertenecen a tipos de datos particulares. Por ejemplo, si un proveedor médico actualiza datos médicos almacenados en el dispositivo cliente 106, puede mostrarse deferencia al proveedor médico sobre el usuario ya que puede asignarse al proveedor médico un nivel de acceso alto 152 por el usuario (o por defecto). En otro ejemplo, si un proveedor médico actualiza información personal, tal como un número de teléfono o dirección para el usuario del dispositivo cliente 106, puede mostrarse deferencia al usuario ya que él o ella está probablemente situado para entender mejor su propio número o dirección. En otras palabras, el proveedor médico puede tener un nivel de acceso alto 152 para información médica y un nivel de acceso bajo 152 para información personal.

Como alternativa, si no existe un conflicto de datos, el proceso continúa a la etapa 1221 en la que, durante procesos de ingestión futuros, los campos en la interfaz de usuarios 131 pueden rellenarse automáticamente con datos obtenidos desde el identificador legible por máquina 133. Posteriormente, el proceso continúa a terminar.

Con referencia a la Figura 13, se muestra un diagrama de flujo que un ejemplo de la operación de una porción de la aplicación de gestión de clave 118 según diversas realizaciones. Se entiende que el diagrama de flujo de la Figura 13 proporciona meramente un ejemplo de los muchos diferentes tipos de disposiciones funcionales que pueden emplearse para implementar la operación de la porción de la aplicación de gestión de clave 118 como se describe en este documento. Como una alternativa, el diagrama de flujo de la Figura 13 puede verse como que representa un ejemplo de elementos de un método implementado en el entorno informático 103 según una o más realizaciones.

Comenzando con 1303, una selección de una entidad, tal como un proveedor médico, se recibe desde un dispositivo cliente 106 en el que se hizo la selección en una aplicación cliente 130. Por ejemplo, el usuario puede especificar una entidad para la que él o ella quiere compartir los datos de entrada proporcionados durante el proceso de ingestión. En un ejemplo, el usuario puede seleccionar el proveedor "Atlanta Health" en una interfaz de usuario 131 generada por la aplicación cliente 130. "Atlanta Health" puede poseer u operar uno o más dispositivos lectores 109 que se asocian con uno o más perfiles de dispositivo 148 almacenados en el almacenamiento de datos 115.

En algunos ejemplos, una entidad, o un perfil de dispositivo 148 que corresponde a un dispositivo lector 109 operado por la entidad, puede tener una clave criptográfica predefinida 121 almacenada en el almacenamiento de datos 115. Sin embargo, en la etapa 1306, puede generarse una clave criptográfica 121 para el perfil de dispositivo 148, por

ejemplo, para crear una clave criptográfica 121 única para la relación usuario a entidad. Como puede apreciarse, la etapa 1306 puede ser opcional. En algunos ejemplos, la clave criptográfica 121 se genera pseudoaleatoriamente, usando información proporcionada por el usuario, o una combinación de los mismos.

A continuación, en la etapa 1309, la clave criptográfica 121 se envía al dispositivo cliente 106 de modo que la aplicación cliente 130 puede codificar los datos de entrada para su recepción por el dispositivo lector 109 asociado con el perfil de dispositivo 148. Si el dispositivo lector 109 no tiene la clave criptográfica 121 almacenada en el mismo, en la etapa 1312, la clave criptográfica 121 puede enviarse al dispositivo lector 109, si se necesita.

Con referencia a la Figura 14, se muestra un diagrama de flujo que muestra otro ejemplo de la operación la aplicación de gestión de clave 118 según diversas realizaciones. Se entiende que el diagrama de flujo de la Figura 14 proporciona meramente un ejemplo de los muchos diferentes tipos de disposiciones funcionales que pueden emplearse para implementar la operación de la porción de la aplicación de gestión de clave 118 como se describe en este documento. Como una alternativa, el diagrama de flujo de la Figura 14 puede verse como que representa un ejemplo de elementos de un método implementado en el entorno informático 103 según una o más realizaciones.

En algunas realizaciones, el identificador legible por máquina 133 puede comprender datos no encriptados o datos que pueden desencriptarse usando una clave criptográfica 121 global o compartida. Los datos pueden incluir un primer identificador de dispositivo 145a para un dispositivo de origen y un segundo identificador de dispositivo 145b para un destinatario previsto. Por ejemplo, una aplicación cliente 130 puede generar un identificador legible por máquina 133 que incluye un primer identificador de dispositivo 145a para el dispositivo cliente 106 que generó el identificador legible por máquina 133a y un segundo identificador de dispositivo 145b para un dispositivo lector 109 de destinatario previsto asociado con una entidad particular, tal como un proveedor médico seleccionado.

Cuando un dispositivo lector 109 escanea el identificador legible por máquina 133, puede determinar si tiene acceso a los datos subyacentes analizando el primer identificador de dispositivo 145a o el segundo identificador de dispositivo 145b para el destinatario previsto. En otros ejemplos, el dispositivo lector 109 puede comunicar los identificadores de dispositivo 145 a la aplicación de gestión de clave 118 para autorización remota. Para este fin, en la etapa 1403, la aplicación de gestión de clave 118 puede recibir un primer identificador de dispositivo 145a para un dispositivo que generó un identificador legible por máquina 133. De manera similar, en la etapa 1406, la aplicación de gestión de clave 118 puede recibir un segundo identificador de dispositivo 145b para un dispositivo destinado para acceder a los datos subyacentes del identificador legible por máquina 133.

Usando el primer identificador de dispositivo 145a y el segundo identificador de dispositivo 145b, la aplicación de gestión de clave 118 puede determinar, en la etapa 1409, si el dispositivo que solicita una clave criptográfica 121 para desencriptar los datos subyacentes del identificador legible por máquina 133 está autorizado para acceder a los datos subyacentes por el usuario originador (por ejemplo, el usuario de la aplicación cliente 130 o el proveedor médico). Si el dispositivo solicitante está autorizado para acceder a los datos subyacentes, en la etapa 1412, la aplicación de gestión de clave 118 puede enviar la clave criptográfica 121 al dispositivo, en el que la clave criptográfica 121 es capaz de desencriptar los datos codificados en el identificador legible por máquina 133. Posteriormente, el proceso continúa a terminar. Haciendo referencia de nuevo a la etapa 1409, si el dispositivo solicitante no está autorizado para acceder a los datos subyacentes del identificador legible por máquina 133, el proceso continúa a terminar.

Las aplicaciones descritas en este documento, tal como la aplicación cliente 130, la aplicación de lector 136, y la aplicación de gestión de clave 118, proporcionan la capacidad de adquirir de forma efectiva, almacenar y reproducir información vital, tal como información requerida en una visita inicial o vista posterior con un proveedor de atención sanitaria. Específicamente, la presente divulgación describe una aplicación cliente 130 para la obtención de un historial médico de una forma intuitiva y generar un identificador legible por máquina 133 que comprende el historial médico obtenido como datos codificados y encriptados. En diversas realizaciones, la información proporcionada por un usuario a través de la aplicación cliente 130 puede almacenarse localmente en el dispositivo cliente 106. La información almacenada en el dispositivo cliente 106 puede encriptarse para almacenamiento local. Adicionalmente, en visitas de regreso, cualquier cambio en la historia clínica puede identificarse fácilmente y proporcionarse al proveedor.

Hoy en día, aplicaciones relacionadas con la salud existentes se centran hacia la ayuda a un individuo en incrementar su capacidad de tomar responsabilidad de su propio cuidado, promocionando una vida saludable y enlazando con sistemas electrónicos de historia clínica a un proveedor o institución para obtener resultados de pruebas y de laboratorio. Estas aplicaciones incluyen diversos grados de puntos de datos diarios o, mejor, semanales que necesitan actualizarse para justificar el uso de la aplicación cliente 130.

La aplicación cliente 130 y la aplicación de lector 136 pueden implementarse en los sistemas operativos de iOS®, Blackberry®, Linux®, Android®, Windows® y/u otros sistemas operativos adecuados. La información obtenida por la aplicación cliente 130 únicamente necesita proporcionarse por un usuario una vez y actualizarse únicamente con cambios significativos y relevantes (por ejemplo, cambios de medicación, procedimientos quirúrgicos) que serán únicamente necesarios de forma infrecuente para la mayoría de pacientes. Además, la aplicación cliente 130 permite

que un usuario proporcione información vital para dependientes o aquellos de los que el usuario puede ser responsable. Como puede apreciarse, el valor de proporcionar fácil y correctamente información básica es enorme.

Según diversas realizaciones, se obtiene una cuenta específica, de bajo mantenimiento y focalizada de información médica esencial que se requiere por proveedores de asistencia sanitaria y otras entidades para proporcionar cuidados rutinarios necesarios. Esta información se genera por médicos con médicos en mente, pero se crean para una navegación fácil del sistema. El flujo de trabajo se creará de una forma que la navegación puede completarse por todos los individuos con solo un nivel de alfabetización básica. En diversas realizaciones, el alcance de información requerido desde un usuario puede pivotar en un número predefinido de cuestiones (por ejemplo, siete cuestiones o algún otro número) que puede ser vital para todas las visitas iniciales a cualquier proveedor de atención sanitaria. En diversas realizaciones, estas cuestiones pueden ser específicas y no abiertas.

La aplicación cliente 130 genera una serie de una o más interfaces de usuario 131 para obtener información desde el usuario. Además, la aplicación cliente 130 correlaciona la información de una forma fácil y legible tanto para el médico como el paciente. Esto también permite la transferencia eficiente de información médica básica entre diversos proveedores, tales como médicos de cabecera y especialistas. La aplicación cliente 130 facilita una correlación de historial médico u otra información para familiares u otros individuos, tales como padres, hijos, mascotas, *etc.* Por ejemplo, la información proporcionada por otro puede ser beneficiosa en situaciones en las que los pacientes son incapaces de proporcionar su propio historial debido a dolor, estrés, confusión, pérdida de consciencia, *etc.,* así como veces en las que un padre está distraído debido a una situación de emergencia. En estos casos, esta información vital puede comunicarse de forma efectiva de forma rápida, fácil y precisa, evitando de este modo errores médicos debido a falta de precisión y de información completa. Además, la aplicación cliente 130 se configura para mejorar la atención sanitaria para aquellos individuos con discapacidades de comunicación, tales como aquellos que son sordos o mudos.

En diversas realizaciones, la consulta de un doctor u otro proveedor de atención sanitaria puede designar información como que es requerida u opcional durante una admisión de cliente. La aplicación cliente 130 se ejecuta para recopilar puntos de datos designados como que son requeridos por los proveedores de asistencia sanitaria. Esta información puede encriptarse según las regulaciones de HIPAA y la Ley de Tecnología de la Información de Salud para la Salud Económica y Clínica ("HITECH") y puede hacerse accesible para el usuario o para proveedores de asistencia sanitaria especificados usando una clave o una contraseña.

Según diversas realizaciones, la información recopilada puede limitarse a lo siguiente: historial médico pasado, historial quirúrgico pasado, alergias, medicaciones, historial familiar, historial social e inmunizaciones, aunque, en otras realizaciones, puede recopilarse información adicional. La aplicación cliente 130 puede ayudar al usuario en la provisión de ortografía correcta para términos médicos básicos y medicaciones para evitar confusión y documentación incorrecta que puede conducir a errores médicos.

La información recopilada por la aplicación cliente 130 puede organizarse en una pantalla de resumen mostrada en una interfaz de usuario 131 para referencia mientras rellena nuevos paquetes de información de paciente. En diversas realizaciones, esta información puede convertirse en un formato de Microsoft Word® o PDF para imprimir antes de una visita con un proveedor de atención sanitaria. Finalmente, esta información puede encriptarse y la información encriptada puede convertirse en un código de matriz u otro identificador legible por máquina 133 para una transferencia sin papel e inalámbrica de información directamente a un proveedor de atención sanitaria. En diversas realizaciones, un escáner del identificador legible por máquina 133 provoca un relleno automático de la información subyacente en una base de datos de diversos sistemas electrónicos de historia clínica.

Además de recopilar información personal, la aplicación cliente 130 puede configurarse para obtener información de salud para dependientes, miembros de la familia, mascotas *etc.* Esto puede ayudar en la provisión a profesionales de la atención sanitaria con información completa y precisa cuando dependientes y miembros de la familia son incapaces de proporcionar esta información por sí mismos debido a la edad, incapacidad, *etc.* Esto puede ayudar al proveedor de asistencia sanitaria a evaluar de forma precisas pacientes, racionalizar la atención y evitar errores médicos debido a historias médicas incompletas. Como se ha indicado anteriormente, la aplicación cliente 130 puede configurarse para obtener información acerca de mascotas, ya que su historial médico es también valioso para propietarios y veterinarios. Siendo capaz de referenciar fácilmente esta información en la misma plataforma ya que el usuario de la aplicación cliente 130, la información puede usarse para la escuela, universidad, viaje internacional, emergencias y otras situaciones.

Aunque esta divulgación proporciona múltiples ejemplos en el contexto de datos de atención sanitaria, las realizaciones adjuntas en este documento son aplicables a través de muchas industrias. Por ejemplo, la información de salud puede incluir información que pertenece a un automóvil. El mecánico puede ver registros de servicio escaneando un identificador legible por máquina 133 presentado en un dispositivo cliente 106, que puede incluir el teléfono inteligente de una persona o un dispositivo informático del automóvil.

Con referencia a la Figura 15, se muestra un diagrama de bloques esquemático del entorno informático 103 según una realización de la presente divulgación. El entorno informático 103 incluye uno o más dispositivos informáticos

1500. Cada dispositivo informático 1500 incluye al menos un circuito de procesador, por ejemplo, que tiene un procesador 1503 y una memoria 1506, ambos de los cuales se acoplan a una interfaz local 1509. Para este fin, cada dispositivo informático 1500 puede comprender, por ejemplo, al menos un ordenador de servidor o dispositivo similar. La interfaz local 1509 puede comprender, por ejemplo, un bus de datos con un bus de control/dirección adjunto u otra estructura de bus como puede apreciarse.

En la memoria 1506 se almacenan tanto datos como varios componentes que son ejecutables por el procesador 1503. En particular, la aplicación de gestión de clave 118, el servicio de traducción 120, el servicio de mensajería directa 122 y otras aplicaciones de entorno informático se almacenan en la memoria 1506 y son ejecutables por el procesador 1503. También pueden almacenarse en la memoria 1506 el almacenamiento de datos 115 y otros datos. Además, un sistema operativo 1512 puede almacenarse en la memoria 1506 y ser ejecutable por el procesador 1503. Se entiende que puede haber otras aplicaciones que se almacenan en la memoria 1506 y son ejecutables por el procesador 1503 como puede apreciarse.

Con referencia a la Figura 16, se muestra un diagrama de bloques esquemático del dispositivo cliente 106 según una realización de la presente divulgación. Cada dispositivo cliente 106 incluye al menos un circuito de procesador, por ejemplo, que tiene un procesador 1603 y una memoria 1606, ambos de los cuales se acoplan a una interfaz local 1609. Para este fin, cada dispositivo cliente 106 puede comprender, por ejemplo, un teléfono inteligente, una tableta, un ordenador personal u otro dispositivo similar. La interfaz local 1609 puede comprender, por ejemplo, un bus de datos con un bus de control/dirección adjunto u otra estructura de bus como puede apreciarse.

En la memoria 1606 se almacenan tanto datos como varios componentes que son ejecutables por el procesador 1603. En particular, la aplicación cliente 130 y otras aplicaciones se almacenan en la memoria 1606 y son ejecutables por el procesador 1603. También en la memoria 1606 pueden almacenarse un almacenamiento de datos de cliente 1612 (también denominado en este documento como un almacenamiento de datos local) y otros datos. Además, un sistema operativo de cliente 1615 puede almacenarse en la memoria 1606 y ser ejecutable por el procesador 1603. Se entiende que puede haber otras aplicaciones que se almacenan en la memoria 1606 y son ejecutables por el procesador 1603 como puede apreciarse.

Con referencia a la Figura 17, se muestra un diagrama de bloques esquemático del dispositivo lector 109 según una realización de la presente divulgación. Cada dispositivo lector 109 incluye al menos un circuito de procesador, por ejemplo, que tiene un procesador 1703 y una memoria 1706, ambos de los cuales se acoplan a una interfaz local 1709. Para este fin, cada dispositivo lector 109 puede comprender, por ejemplo, un teléfono inteligente, una tableta, un ordenador personal u otro dispositivo similar. La interfaz local 1709 puede comprender, por ejemplo, un bus de datos con un bus de control/dirección adjunto u otra estructura de bus como puede apreciarse.

En la memoria 1706 se almacenan tanto datos como varios componentes que son ejecutables por el procesador 1703. En particular, la aplicación de lector 136 y otras aplicaciones se almacenan en la memoria 1706 y son ejecutables por procesador 1703. También en la memoria 1706 pueden almacenarse un almacenamiento de datos de lector 1712 y otros datos. Además, un sistema operativo de cliente 1715 puede almacenarse en la memoria 1706 y ser ejecutable por el procesador 1703. Se entiende que puede haber otras aplicaciones que se almacenan en la memoria 1706 y son ejecutables por el procesador 1703 como puede apreciarse.

Donde cualquier componente analizado en este documento se implementa en forma de software, puede emplearse uno cualquiera de un número de lenguajes de programación, tales como, por ejemplo, C, C++, C#, Objective C, Java®, JavaScript®, Perl, PHP, Visual Basic®, Python®, Ruby, Flash®, Swift® u otros lenguajes de programación.

Un número de componentes de software se almacenan en la memoria ejecutable por los procesadores. A este respecto, el término "ejecutable" significa un archivo de programa que es en una forma que puede ejecutarse finalmente por los procesadores. Ejemplos de programas ejecutables pueden ser, por ejemplo, un programa compilado que puede trasladarse en código máquina en un formato que puede cargarse en una porción de acceso aleatorio de la memoria y ejecutarse por un procesador, código fuente que puede expresarse en un formato apropiado tal como código objeto que es capaz de cargarse en una porción de acceso aleatorio de memoria y ejecutarse por un procesador, código fuente que puede interpretarse por otro programa ejecutable para generar instrucciones en una porción de acceso aleatorio de la memoria a ejecutarse por un procesador, *etc.* Un programa ejecutable puede almacenarse en cualquier porción o componente de la memoria que incluye, por ejemplo, memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), disco duro, unidad de estado sólido, unidad flash de USB, tarjeta de memoria, disco óptico tal como disco compacto (CD) o disco versátil digital (DVD), disco flexible, cinta magnética u otras memorias de memoria.

La memoria se define en este documento como que incluye memoria volátil y no volátil y componentes de almacenamiento de datos. Componentes volátiles son los que no retienen valores de datos tras la pérdida de potencia. Componentes no volátiles son los que retienen datos tras una pérdida de potencia. Por lo tanto, la memoria puede comprender, por ejemplo, memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), unidades de disco duro, unidades de estado sólido, unidades flash de USB, tarjetas de memoria accedidas a través de un lector de tarjeta de memoria, discos flexibles accedidos a través de una unidad de disco flexible asociada, discos ópticos

accedidos a través de una unidad de disco óptico, cintas magnéticas accedidos a través de una unidad de cinta apropiada y/u otros componentes de memoria, o una combinación de dos cualesquiera o más de estos componentes de memoria. Además, la RAM puede comprender, por ejemplo, memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM) o memoria de acceso aleatorio magnética (MRAM) y otros tales dispositivos. La ROM puede comprender, por ejemplo, una memoria de sólo lectura programable (PROM), una memoria de sólo lectura borrable y programable (EPROM), una memoria de sólo lectura eléctricamente programable borrable (EEP-ROM) u otro dispositivo de memoria similar.

También, el procesador puede representar múltiples procesadores y/o múltiples núcleos de procesadores y la memoria puede representar múltiples memorias que operan en circuitos de procesamiento paralelos, respectivamente. En un caso de este tipo, la interfaz local puede ser una red apropiada que facilita comunicación entre dos cualesquiera de los múltiples procesadores, entre cualquier procesador y cualquiera de las memorias, o entre dos cualesquiera de las memorias, *etc.* La interfaz local puede comprender sistemas adicionales diseñados para coordinar esta comunicación, incluyendo, por ejemplo, realizar equilibrio de carga. El procesador puede ser de construcción eléctrica o de alguna otra construcción disponible.

Aunque la aplicación cliente 130, la aplicación de lector 136, la aplicación de gestión de clave 118 y otros diversos sistemas descritos en este documento puede incorporarse en software o código ejecutado por hardware de fin general como se ha analizado anteriormente, como una alternativa lo mismo también puede incorporarse en hardware especializado o una combinación de software/hardware de fin general y hardware especializado. Si se incorpora en hardware especializado, cada uno puede implementarse como un circuito o máquina de estados que emplea uno cualquiera de o una combinación de un número de tecnologías. Estas tecnologías pueden incluir, pero sin limitación, circuitos lógicos discretos que tienen puertas lógicas para implementar diversas funciones lógicas tras una aplicación de una o más señales de datos, circuitos integrados específicos de la aplicación (ASIC) que tienen puertas lógicas apropiadas, campos de matrices de puertas programables (FPGA) u otros componentes, *etc.* Tales tecnologías se conocen bien generalmente por los expertos en la materia y, en consecuencia, no se describen en detalle en este documento.

Los diagramas de flujo de las Figuras 6 y 10-14 muestran la funcionalidad y operación de una implementación de porciones de la aplicación cliente 130, la aplicación de lector 136 y la aplicación de gestión de clave 118. Si se incorpora en software, cada bloque puede representar un módulo, segmento o porción de código que comprende instrucciones de programa para implementar la función o funciones lógicas especificadas. Las instrucciones de programa pueden incorporarse en forma de código fuente que comprende sentencias legibles por humanos escritas en un lenguaje de programación o código máquina que comprende instrucciones numéricas reconocibles por un sistema de ejecución adecuado tal como un procesador en un sistema informático u otro sistema. El código máquina puede convertirse a partir del código fuente, *etc.* Si se incorpora en hardware, cada bloque puede representar un circuito o un número de circuitos interconectados para implementar la función o funciones lógicas especificadas.

Aunque los diagramas de flujo de las Figuras 6 y 10-14 muestran un orden específico de ejecución, se entiende que el orden de ejecución puede diferir de lo que se representa. Por ejemplo, el orden de ejecución de dos o más bloques puede aleatorizarse en relación con el orden mostrado. También, dos o más bloques mostrados en sucesión en las Figuras 6 y 10-14 pueden ejecutarse simultáneamente o con concurrencia parcial. Además, en algunas realizaciones, uno o más de los bloques mostrados en las Figuras 6 y 10-14 pueden saltarse u omitirse. Además, cualquier número de contadores, variables de estado, semáforos de aviso o mensajes podría añadirse al flujo lógico descrito en este documento, para propósitos de utilizad mejorada, contabilidad, medición de rendimiento o provisión de ayudas a la resolución de problemas, *etc.* Se entiende que todas tales variaciones están dentro del alcance de la presente divulgación.

También, cualquier lógica o aplicación descrita en este documento, incluyendo la aplicación cliente 130, la aplicación de lector 136 y la aplicación de gestión de clave 118 que comprende software o código puede incorporarse en cualquier medio legible por ordenador no transitorio para su uso por o en conexión con un sistema de ejecución de instrucciones tal como, por ejemplo, un procesador en un sistema informático u otro sistema. En este sentido, la lógica puede comprender, por ejemplo, sentencias que incluyen instrucciones y declaraciones que pueden buscarse desde el medio legible por ordenador y ejecutarse por el sistema de ejecución de instrucciones. En el contexto de la presente divulgación, un "medio legible por ordenador" puede ser cualquier medio que puede contener, almacenar o mantener la lógica o aplicación descrita en este documento para su uso por o en conexión con el sistema de ejecución de instrucciones.

El medio legible por ordenador puede comprender uno cualquiera de muchos medios físicos tales como, por ejemplo, medios magnéticos, ópticos o de semiconductor. Más ejemplos específicos de un medio legible por ordenador adecuado incluiría, pero sin limitación, cintas magnéticas, discos flexibles magnéticos, discos duros magnéticos, tarjetas de memoria, unidades de estado sólido, unidades flash de USB o discos ópticos. También, el medio legible por ordenador puede ser una memoria de acceso aleatorio (RAM) que incluye, por ejemplo, memoria de acceso aleatorio estática (SRAM) y memoria de acceso aleatorio dinámica (DRAM) o memoria de acceso aleatorio magnética (MRAM). Además, el medio legible por ordenador puede ser una memoria de sólo lectura (ROM), una memoria de sólo lectura programable (PROM), una memoria de sólo lectura borrable y programable

(EPROM), una memoria de sólo lectura eléctricamente programable borrable (EEPROM) u otro tipo de dispositivo de memoria.

Además, cualquier lógica o aplicación descrita en este documento, la aplicación cliente 130, la aplicación de lector 136 y la aplicación de gestión de clave 118 pueden implementarse y estructurarse en una diversidad de formas. Por ejemplo, una o más aplicaciones descritas pueden implementarse como módulos o componentes de una única operación. Además, una o más aplicaciones descritas en este documento pueden ejecutarse en dispositivos informáticos compartidos o separados o una combinación de los mismos. Por ejemplo, una pluralidad de las aplicaciones descritas en este documento pueden ejecutarse en el mismo dispositivo informático 1500 o en múltiples dispositivos informáticos en el mismo entorno informático 103. Adicionalmente, se entiende que términos tales como "aplicación", "servicio", "sistema", "motor", "módulo" y así sucesivamente pueden ser intercambiables y no pretenden ser limitantes.

Lenguaje disyuntivo tal como la frase "al menos uno de X, Y o Z", a no ser que se indique específicamente de otra manera, se entiende de otra manera con el contexto según se usan en general para presentar que un artículo, término, etc., puede ser o bien X, Y o bien Z o cualquier combinación de los mismos (por ejemplo, X, Y y/o Z). Por lo tanto, tal lenguaje disyuntivo no pretende generalmente, y no debería, implicar que ciertas realizaciones requieren que al menos uno de X, al menos uno de Y o al menos uno de Z esté cada uno presente.

Debería destacarse que las realizaciones anteriormente descritas de la presente divulgación son meramente posibles ejemplos de implementaciones expuestas para un claro entendimiento de los principios de la divulgación.

Cláusula 1. Un sistema, que comprende: un dispositivo cliente que comprende al menos un procesador de hardware; una aplicación cliente ejecutable en el dispositivo cliente que comprende instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente: reciba una primera clave criptográfica asociada con un primer perfil de dispositivo y una segunda clave criptográfica asociada con un segundo perfil de dispositivo a través de una red; acceda a datos de entrada desde un almacenamiento de datos del dispositivo cliente, los datos de entrada proporcionados a través de al menos una interfaz de usuario generada por la aplicación cliente; formatee los datos de entrada en al menos una primera porción de datos y una segunda porción de datos; encripte la primera porción de datos usando la primera clave criptográfica y la segunda porción de datos usando la segunda clave criptográfica; y genere un identificador legible por máquina usando la primera porción de datos encriptados y la segunda porción de datos encriptados para representar en un visualizador accesible por el dispositivo cliente.

Cláusula 2. El sistema de la cláusula 1, en el que el identificador legible por máquina es un primer identificador legible por máquina y la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente: identifique un segundo identificador legible por máquina en una imagen capturada por una cámara en comunicación con el dispositivo cliente, generándose el segundo identificador legible por máquina por un dispositivo diferente que el dispositivo cliente; identifique una cantidad de datos encriptados a partir del segundo identificador legible por máquina; desencripte la cantidad de datos encriptados para identificar datos desencriptados usando la primera clave criptográfica o la segunda clave criptográfica; y almacene los datos desencriptados en el almacenamiento de datos para su acceso por la aplicación cliente.

Cláusula 3. El sistema de la cláusula 2, en el que almacenar los datos desencriptados en el almacenamiento de datos comprende, además: identificar si existe un conflicto entre los datos de entrada almacenados en el almacenamiento de datos y los datos desencriptados; y almacenar los datos desencriptados en lugar de los datos de entrada almacenados en el almacenamiento de datos.

Cláusula 4. El sistema de la cláusula 1, comprendiendo adicionalmente: un primer dispositivo lector asociado con el primer perfil de dispositivo que tiene la primera clave criptográfica almacenada en el mismo; un segundo dispositivo lector asociado con el segundo perfil de dispositivo que tiene la segunda clave criptográfica almacenada en el mismo; y en el que el primer dispositivo lector se configura para acceder a la primera porción de datos desde el identificador legible por máquina usando la primera clave criptográfica y el segundo dispositivo lector se configura para acceder a la segunda porción de datos desde el identificador legible por máquina usando la segunda clave criptográfica.

Cláusula 5. El sistema de la cláusula 4, en el que el primer dispositivo lector comprende un primer dispositivo de formación de imágenes y el segundo dispositivo lector comprende un segundo dispositivo de formación de imágenes, capturándose el identificador legible por máquina por el primer dispositivo de formación de imágenes o el segundo dispositivo de formación de imágenes.

Cláusula 6. El sistema de la cláusula 1, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente envíe el identificador legible por máquina a otro dispositivo cliente diferente del dispositivo cliente.

Cláusula 7. El sistema de la cláusula 1, en el que el identificador legible por máquina se genera usando una cantidad de datos desencriptados de los datos de entrada.

Cláusula 8. El sistema de la cláusula 1, en el que la primera clave criptográfica asociada con el primer perfil de dispositivo se recibe por el dispositivo cliente desde al menos un dispositivo informático remoto a través de la red en respuesta a una selección del primer perfil de dispositivo hecha en el dispositivo cliente; y en el que la segunda clave criptográfica asociada con el segundo perfil de dispositivo se recibe por el dispositivo cliente

desde al menos un dispositivo informático remoto a través de la red en respuesta a una selección del segundo perfil de dispositivo hecha en el dispositivo cliente.

Cláusula 9. El sistema de la cláusula 1, en el que encriptar la primera porción de datos usando la primera clave criptográfica y la segunda porción de datos usando la segunda clave criptográfica comprende además: identificar un primer nivel de acceso asociado con la primera porción de datos; identificar un segundo nivel de acceso asociado con la segunda porción de datos; encriptar la primera porción de datos usando la primera clave criptográfica basándose al menos en parte en el primer nivel de acceso; y encriptar la segunda porción de datos usando la segunda clave criptográfica basándose al menos en parte en el segundo nivel de acceso, en el que el primer nivel de acceso es diferente que el segundo nivel de acceso.

Cláusula 10. El sistema de la cláusula 1, en el que el identificador legible por máquina es un código de respuesta rápida (QR) o un código de barras.

Cláusula 11. Un método implementado por ordenador, que comprende: recibir, por un dispositivo cliente que comprende al menos un procesador de hardware, una primera clave criptográfica asociada con un primer perfil de dispositivo y una segunda clave criptográfica asociada con un segundo perfil de dispositivo a través de una red; acceder, por el dispositivo cliente, a datos de entrada desde un almacenamiento de datos del dispositivo cliente, los datos de entrada proporcionados a través de al menos una interfaz de usuario generada por una aplicación cliente ejecutable en el dispositivo cliente; formatear, por el dispositivo cliente, los datos de entrada en al menos una primera porción de datos y una segunda porción de datos; encriptar, por el dispositivo cliente, la primera porción de datos usando la primera clave criptográfica y la segunda porción de datos usando la segunda clave criptográfica; y generar, por el dispositivo cliente, un identificador legible por máquina usando la primera porción de datos encriptados y la segunda porción de datos encriptados para representar en un visualizador accesible por el dispositivo cliente.

Cláusula 12. El método implementado por ordenador de la cláusula 11, en el que el identificador legible por máquina es un primer identificador legible por máquina y el método comprende adicionalmente: identificar, por el dispositivo cliente, un segundo identificador legible por máquina en una imagen capturada por una cámara en comunicación con el dispositivo cliente, generándose el segundo identificador legible por máquina por un dispositivo diferente que el dispositivo cliente; identificar, por el dispositivo cliente, una cantidad de datos encriptados desde el segundo identificador legible por máquina; desencriptar, por el dispositivo cliente, la cantidad de datos encriptados para identificar datos desencriptados usando la primera clave criptográfica o la segunda clave criptográfica; y almacenar, por el dispositivo cliente, los datos desencriptados en el almacenamiento de datos para su acceso por una aplicación cliente.

Cláusula 13. El método implementado por ordenador de la cláusula 12, en el que almacenar los datos desencriptados en el almacenamiento de datos comprende, además: identificar, por el dispositivo cliente, si existe un conflicto entre los datos de entrada almacenados en el almacenamiento de datos y los datos desencriptados; y almacenar, por el dispositivo cliente, los datos desencriptados en lugar de los datos de entrada almacenados en el almacenamiento de datos.

Cláusula 14. El método implementado por ordenador de la cláusula 11, comprendiendo adicionalmente: acceder, por un primer dispositivo lector, la primera porción de datos desde el identificador legible por máquina usando la primera clave criptográfica, asociándose el primer dispositivo lector con el primer perfil de dispositivo y teniendo la primera clave criptográfica almacenada en el mismo; y acceder, por un segundo dispositivo lector, la segunda porción de datos desde el identificador legible por máquina usando la segunda clave criptográfica, asociándose el segundo dispositivo lector con el segundo perfil de dispositivo y teniendo la segunda clave criptográfica almacenada en el mismo.

Cláusula 15. El método implementado por ordenador de la cláusula 14, en el que el primer dispositivo lector comprende un primer dispositivo de formación de imágenes y el segundo dispositivo lector comprende un segundo dispositivo de formación de imágenes, capturándose el identificador legible por máquina por el primer dispositivo de formación de imágenes o el segundo dispositivo de formación de imágenes.

Cláusula 16. El método implementado por ordenador de la cláusula 11, comprendiendo adicionalmente enviar, por el dispositivo cliente, el identificador legible por máquina a otro dispositivo cliente diferente del dispositivo cliente a través de la red.

Cláusula 17. El método implementado por ordenador de la cláusula 11, en el que el identificador legible por máquina se genera usando una cantidad de datos desencriptados de los datos de entrada.

Cláusula 18. El método implementado por ordenador de la cláusula 11, en el que la primera clave criptográfica asociada con el primer perfil de dispositivo se recibe por el dispositivo cliente desde al menos un dispositivo informático remoto a través de la red en respuesta a una selección del primer perfil de dispositivo hecha en el dispositivo cliente; y en el que la segunda clave criptográfica asociada con el segundo perfil de dispositivo se recibe por el dispositivo cliente desde al menos un dispositivo informático remoto a través de la red en respuesta a una selección del segundo perfil de dispositivo hecha en el dispositivo cliente.

Cláusula 19. El método implementado por ordenador de la cláusula 11, en el que encriptar la primera porción de datos usando la primera clave criptográfica y la segunda porción de datos usando la segunda clave criptográfica comprende además: identificar, por el dispositivo cliente, un primer nivel de acceso asociado con la primera porción de datos; identificar, por el dispositivo cliente, un segundo nivel de acceso asociado con la segunda porción de datos; encriptar, por el dispositivo cliente, la primera porción de datos usando la primera clave criptográfica basándose al menos en parte en el primer nivel de acceso; y encriptar, por el dispositivo cliente, la segunda porción de datos usando la segunda clave criptográfica basándose al menos en parte en el segundo nivel de acceso, en el que el primer nivel de acceso es diferente que el segundo nivel de acceso.

Cláusula 20. El método implementado por ordenador de la cláusula 11, en el que el identificador legible por máquina es un código de respuesta rápida (QR) o un código de barras.

Cláusula 21. Un sistema, que comprende: un dispositivo cliente que comprende al menos un procesador de hardware; una aplicación cliente ejecutable en el dispositivo cliente que comprende instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente: genere un primer identificador legible por máquina usando una primera cantidad de datos encriptados usando al menos una clave criptográfica para representar en un visualizador del dispositivo cliente, en el que un dispositivo lector que tiene la al menos una clave criptográfica almacenada en el mismo se configura para desencriptar los datos; identifique un segundo identificador legible por máquina en al menos una imagen capturada por el dispositivo cliente; decodifique el segundo identificador legible por máquina para identificar una segunda cantidad de datos encriptados por el dispositivo lector usando la al menos una clave criptográfica; desencripte la segunda cantidad de datos usando la al menos una clave criptográfica; e identifique si existe un conflicto entre la primera cantidad de datos y la segunda cantidad de datos.

Cláusula 22. El sistema de la cláusula 21, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente, en respuesta al conflicto existente entre la primera cantidad de datos y la segunda cantidad de datos, realice una tarea para resolver el conflicto.

Cláusula 23. El sistema de la cláusula 21, en el que el conflicto se identifica en respuesta al dispositivo lector alterando la primera cantidad de datos para generar la segunda cantidad de datos.

Cláusula 24. El sistema de la cláusula 22, en el que la tarea comprende: presentar información asociada con el conflicto en una interfaz de usuario de la aplicación cliente; recibir una selección de la primera cantidad de datos o la segunda cantidad de datos en la interfaz de usuario; y en respuesta a la selección, actualizar un almacenamiento de datos del dispositivo cliente con la primera cantidad de datos seleccionados o la segunda cantidad de datos seleccionados.

Cláusula 25. El sistema de la cláusula 22, en el que la tarea comprende actualizar un almacenamiento de datos del dispositivo cliente con la segunda cantidad de datos.

Cláusula 26. El sistema de la cláusula 21, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente rellene al menos un campo de una interfaz de usuario en la aplicación cliente con al menos una porción de la segunda cantidad de datos.

Cláusula 27. El sistema de la cláusula 21, en el que la primera cantidad de datos encriptados usando al menos una clave criptográfica comprende además una primera porción de entrada de usuario y una segunda porción de entrada de usuario obtenida durante un proceso de ingestión, encriptándose la primera porción de entrada de usuario usando una primera clave criptográfica accesible por el dispositivo lector y encriptándose la segunda porción de entrada de usuario usando una segunda clave criptográfica no accesible por el dispositivo lector.

Cláusula 28. El sistema de la cláusula 21, en el que el identificador legible por máquina es un código de respuesta rápida (QR) o un código de barras.

Cláusula 29. El sistema de la cláusula 21, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente reciba al menos una clave criptográfica desde una aplicación ejecutándose en un entorno informático remoto a través de una red.

Cláusula 30. El sistema de la cláusula 29, en el que la aplicación remota que se ejecuta en el entorno informático remoto se configura para enviar la al menos una clave criptográfica al dispositivo lector a través de la red.

Cláusula 31. Un método implementado por ordenador, que comprende: generar, por un dispositivo cliente que comprende al menos un procesador de hardware, un primer identificador legible por máquina usando una primera cantidad de datos encriptados usando al menos una clave criptográfica para representar en un visualizador del dispositivo cliente, en el que un dispositivo lector que tiene la al menos una clave criptográfica almacenada en el mismo se configura para desencriptar los datos; identificar, por el dispositivo cliente, un segundo identificador legible por máquina en al menos una imagen capturada por el dispositivo cliente; decodificar, por el dispositivo cliente, el segundo identificador legible por máquina para identificar una segunda cantidad de datos encriptados por el dispositivo lector usando la al menos una clave criptográfica; desencriptar, por el dispositivo cliente, la segunda cantidad de datos usando la al menos una clave criptográfica; e identificar, por el dispositivo cliente, si existe un conflicto entre la primera cantidad de datos y la segunda cantidad de datos.

Cláusula 32. El método implementado por ordenador de la cláusula 31, comprendiendo adicionalmente, en respuesta al conflicto existente entre la primera cantidad de datos y la segunda cantidad de datos, realizar, por el dispositivo cliente, una tarea para resolver el conflicto.

Cláusula 33. El método implementado por ordenador de la cláusula 31, en el que el conflicto se identifica en respuesta al dispositivo lector alterando la primera cantidad de datos para generar la segunda cantidad de datos.

Cláusula 34. El método implementado por ordenador de la cláusula 32, en el que la tarea comprende: presentar, por el dispositivo cliente, información asociada con el conflicto en una interfaz de usuario de la aplicación cliente; identificar, por el dispositivo cliente, una selección de la primera cantidad de datos o la segunda cantidad de datos hecha en la interfaz de usuario; y en respuesta a la selección identificándose, actualizar, por el dispositivo cliente, un almacenamiento de datos del dispositivo cliente con la primera cantidad de datos seleccionados o la segunda cantidad de datos seleccionados.

Cláusula 35. El método implementado por ordenador de la cláusula 32, en el que la tarea comprende actualizar, por el dispositivo cliente, un almacenamiento de datos del dispositivo cliente con la segunda cantidad de datos.

Cláusula 36. El método implementado por ordenador de la cláusula 31, comprendiendo adicionalmente rellenar, por el dispositivo cliente, al menos un campo de una interfaz de usuario en una aplicación cliente con al menos una porción de la segunda cantidad de datos.

Cláusula 37. El método implementado por ordenador de la cláusula 31, en el que la primera cantidad de datos encriptados usando al menos una clave criptográfica comprende además una primera porción de entrada de usuario y una segunda porción de entrada de usuario obtenida durante un proceso de ingestión, encriptándose la primera porción de entrada de usuario usando una primera clave criptográfica accesible por el dispositivo lector y encriptándose la segunda porción de entrada de usuario usando una segunda clave criptográfica no accesible por el dispositivo lector.

Cláusula 38. El método implementado por ordenador de la cláusula 31, en el que el identificador legible por máquina es un código de respuesta rápida (QR) o un código de barras.

Cláusula 39. El método implementado por ordenador de la cláusula 31, comprendiendo adicionalmente recibir, por el dispositivo cliente, al menos una clave criptográfica desde una aplicación ejecutándose en un entorno informático remoto a través de una red.

Cláusula 40. El método implementado por ordenador de la cláusula 39, en el que la aplicación remota que se ejecuta en el entorno informático remoto se configura para enviar la al menos una clave criptográfica al dispositivo lector a través de la red.

**REIVINDICACIONES**

1. Un sistema, que comprende:

un dispositivo cliente que comprende al menos un procesador de hardware;
una aplicación cliente ejecutable en el dispositivo cliente que comprende instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente:

genere un primer identificador legible por máquina usando una primera cantidad de datos encriptados usando al menos una clave criptográfica para representar en un visualizador del dispositivo cliente, en el que un dispositivo lector que tiene la al menos una clave criptográfica almacenada en el mismo se configura para desencriptar la primera cantidad de datos, comprendiendo la primera cantidad de datos una primera porción de entrada de usuario y una segunda porción de entrada de usuario, encriptándose la primera porción de entrada de usuario usando una primera clave criptográfica que es accesible por el dispositivo lector y encriptándose la segunda porción de entrada de usuario usando una segunda clave criptográfica que no es accesible por el dispositivo lector;
identifique un segundo identificador legible por máquina en al menos una imagen capturada por el dispositivo cliente, generándose el segundo identificador legible por máquina por el dispositivo lector;
decodifique el segundo identificador legible por máquina para identificar una segunda cantidad de datos creada por el dispositivo lector, después de que la primera cantidad de datos se desencripta usando la al menos una clave criptográfica, basándose al menos en parte en la primera cantidad de datos y desencriptada por el dispositivo lector usando la al menos una clave criptográfica;
desencripte la segunda cantidad de datos usando la al menos una clave criptográfica; e
identifique si existe un conflicto entre la primera cantidad de datos y la segunda cantidad de datos.

2. El sistema de la reivindicación 1, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente, en respuesta al conflicto existente entre la primera cantidad de datos y la segunda cantidad de datos, realice una tarea para resolver el conflicto.

3. El sistema de la reivindicación 2, en el que la tarea comprende al menos una de:

presentar información asociada con el conflicto en una interfaz de usuario de la aplicación cliente; recibir una selección de la primera cantidad de datos o la segunda cantidad de datos en la interfaz de usuario; y
en respuesta a la selección, actualizar un almacenamiento de datos del dispositivo cliente con la primera cantidad de datos seleccionados o la segunda cantidad de datos seleccionados.

4. El sistema de la reivindicación 3, en el que la tarea comprende además actualizar un almacenamiento de datos del dispositivo cliente con la segunda cantidad de datos.

5. El sistema de la reivindicación 1, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente rellene al menos un campo de una interfaz de usuario en la aplicación cliente con al menos una porción de la segunda cantidad de datos.

6. El sistema de la reivindicación 1, en el que la primera porción de entrada de usuario y la segunda porción de entrada de usuario se obtienen durante un proceso de ingestión.

7. El sistema de la reivindicación 1, en el que la aplicación cliente comprende además instrucciones de programa que, cuando se ejecutan, provocan que el dispositivo cliente reciba al menos una clave criptográfica desde una aplicación ejecutándose en un entorno informático remoto a través de una red.

8. Un método implementado por ordenador, que comprende:

generar, por un dispositivo cliente que comprende al menos un procesador de hardware, un primer identificador legible por máquina usando una primera cantidad de datos encriptados usando al menos una clave criptográfica para representar en un visualizador del dispositivo cliente, en el que un dispositivo lector que tiene la al menos una clave criptográfica almacenada en el mismo se configura para desencriptar la primera cantidad de datos, comprendiendo la primera cantidad de datos una primera porción de entrada de usuario y una segunda porción de entrada de usuario, encriptándose la primera porción de entrada de usuario usando una primera clave criptográfica que es accesible por el dispositivo lector y encriptándose la segunda porción de entrada de usuario usando una segunda clave criptográfica que no es accesible por el dispositivo lector;
identificar, por el dispositivo cliente, un segundo identificador legible por máquina en al menos una imagen capturada por el dispositivo cliente, generándose el segundo identificador legible por máquina por el dispositivo lector;
decodificar, por el dispositivo cliente, el segundo identificador legible por máquina para identificar una segunda cantidad de datos creada por el dispositivo lector, después de que la primera cantidad de datos se desencripta usando la al menos una clave criptográfica, basándose al menos en parte en la primera cantidad de datos y

desencriptada por el dispositivo lector usando la al menos una clave criptográfica;
desencriptar, por el dispositivo cliente, la segunda cantidad de datos usando la al menos una clave criptográfica; e
identificar, por el dispositivo cliente, si existe un conflicto entre la primera cantidad de datos y la segunda cantidad de datos.

9. El método implementado por ordenador de la reivindicación 8, que comprende adicionalmente, en respuesta al conflicto existente entre la primera cantidad de datos y la segunda cantidad de datos, realizar, por el dispositivo cliente, una tarea para resolver el conflicto.

10. El método implementado por ordenador de la reivindicación 9, en el que la tarea comprende al menos una de:

presentar información asociada con el conflicto en una interfaz de usuario de la aplicación cliente; recibir una selección de la primera cantidad de datos o la segunda cantidad de datos en la interfaz de usuario; y
en respuesta a la selección, actualizar un almacenamiento de datos del dispositivo cliente con la primera cantidad de datos seleccionados o la segunda cantidad de datos seleccionados.

11. El método implementado por ordenador de la reivindicación 10, en el que la tarea comprende además actualizar un almacenamiento de datos del dispositivo cliente con la segunda cantidad de datos.

12. El método implementado por ordenador de la reivindicación 8, que comprende adicionalmente rellenar, por el dispositivo cliente, al menos un campo de una interfaz de usuario en la aplicación cliente con al menos una porción de la segunda cantidad de datos.

13. El método implementado por ordenador de la reivindicación 8, en el que la primera porción de entrada de usuario y la segunda porción de entrada de usuario se obtienen durante un proceso de ingestión.

14. El método implementado por ordenador de la reivindicación 8, comprendiendo adicionalmente recibir, por el dispositivo cliente, al menos una clave criptográfica desde una aplicación ejecutándose en un entorno informático remoto a través de una red.

15. El método implementado por ordenador de la reivindicación 8, en el que el identificador legible por máquina es un código de respuesta rápida (QR) o un código de barras.

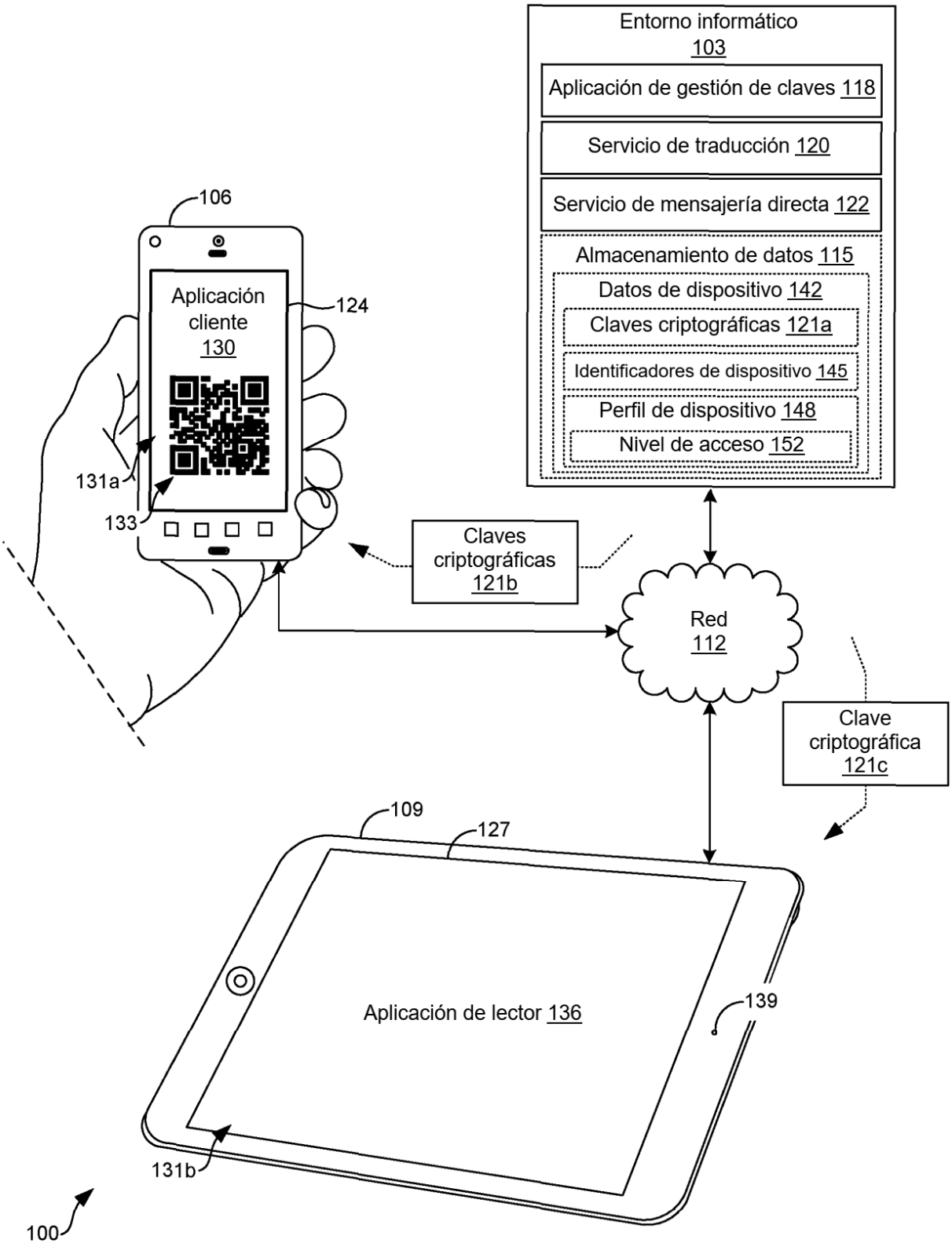
Entorno informático
103
Aplicación de gestión de claves 118
Servicio de traducción 120
Servicio de mensajería directa 122
Almacenamiento de datos 115
Datos de dispositivo 142
Claves criptográficas 121a
Identificadores de dispositivo 145
Perfil de dispositivo 148
Nivel de acceso 152
106
Aplicación cliente 130
124
131a
133
Claves criptográficas 121b
Red 112
Clave criptográfica 121c
109
127
Aplicación de lector 136
139
131b
100

FIG. 1

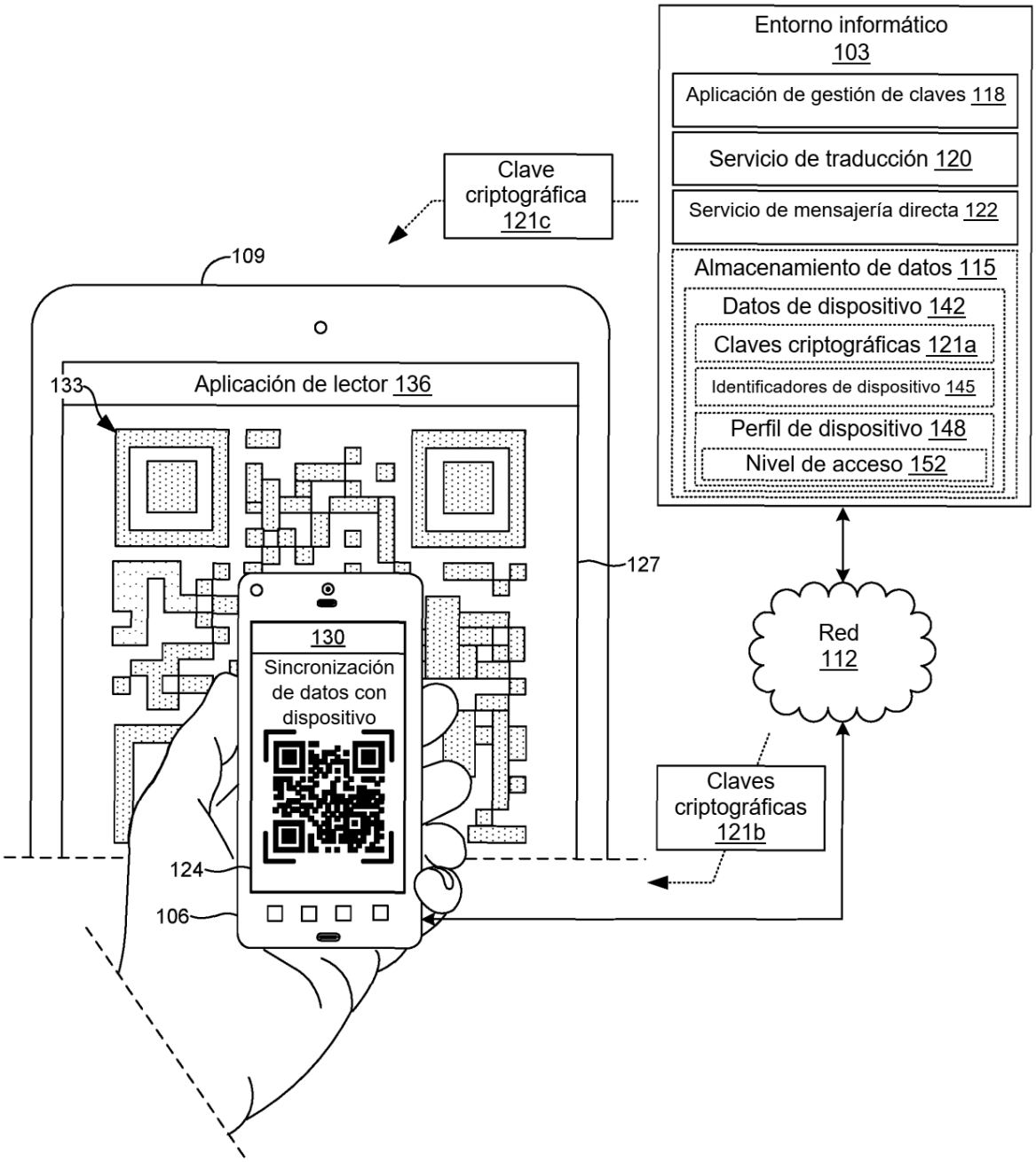
Entorno informático
103
Aplicación de gestión de claves 118
Servicio de traducción 120
Servicio de mensajería directa 122
Almacenamiento de datos 115
Datos de dispositivo 142
Claves criptográficas 121a
Identificadores de dispositivo 145
Perfil de dispositivo 148
Nivel de acceso 152
Clave criptográfica 121c
109
133
Aplicación de lector 136
127
130
Sincronización de datos con dispositivo
Red 112
Claves criptográficas 121b
124
106

FIG. 2

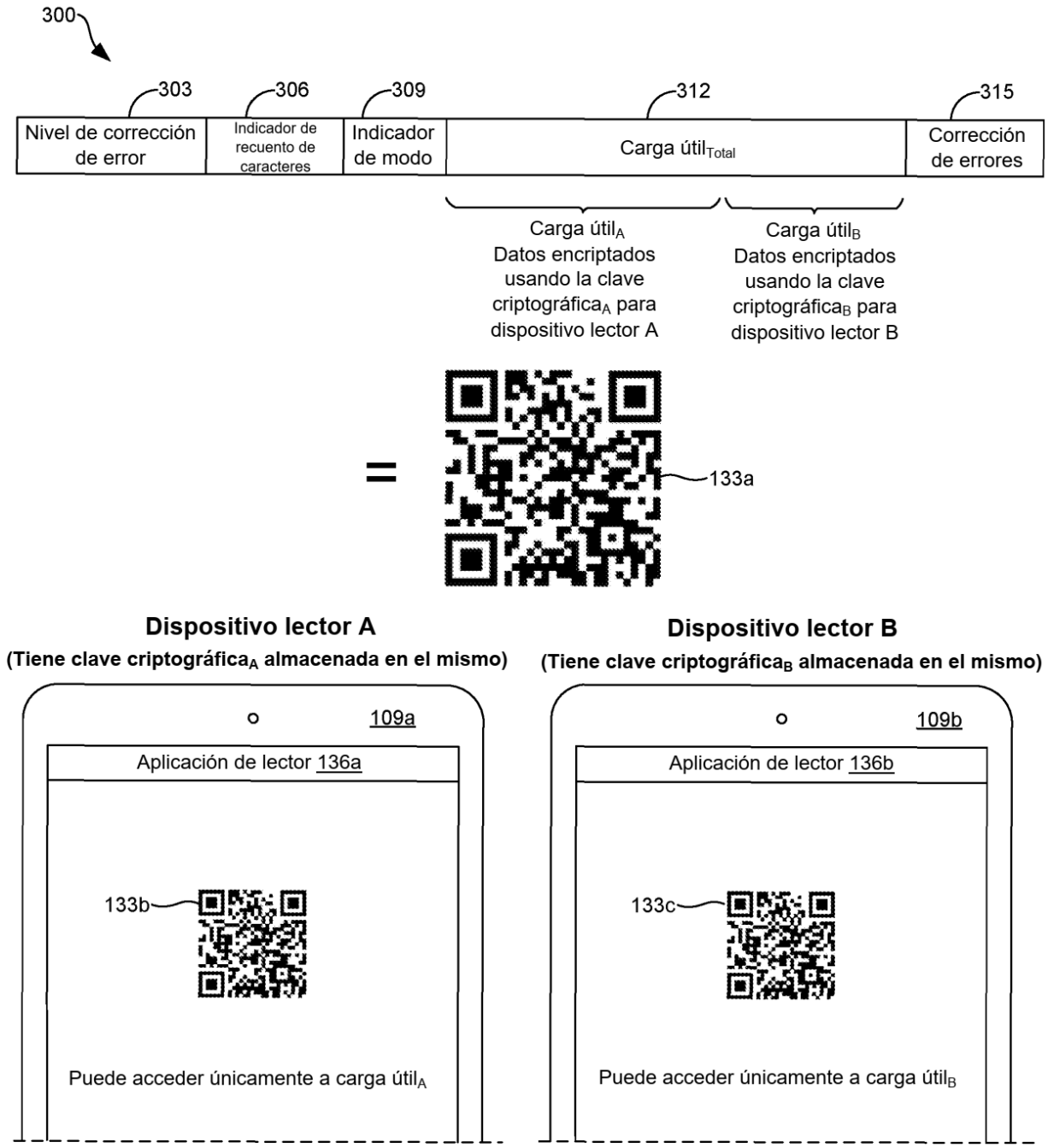
300
303
306
309
312
315
Nivel de corrección de error
Indicador de recuento de caracteres
Indicador de modo
Carga útil Total
Corrección de errores
Carga útil A
Datos encriptados usando la clave criptográfica A para dispositivo lector A
Carga útil B
Datos encriptados usando la clave criptográfica B para dispositivo lector B
=
133a
Dispositivo lector A
(Tiene clave criptográfica A almacenada en el mismo)
109a
Aplicación de lector 136a
133b
Puede acceder únicamente a carga útil A
Dispositivo lector B
(Tiene clave criptográfica B almacenada en el mismo)
109b
Aplicación de lector 136b
133c
Puede acceder únicamente a carga útil B

FIG. 3

**Capacidad de Código de Matriz de Versión 40-L**

| Modo de codificación | Indicador de modo |
|---|---|
| Numérico | 7089 Caracteres |
| Alfanumérico | 4296 Caracteres |
| Byte | 2953 Caracteres |
| Kanji | 1817 Caracteres |

FIG. 4

| Nombre de modo | Indicador de modo |
|---|---|
| Numérico | 0001 |
| Alfanumérico | 0010 |
| Byte | 0100 |
| Kanji | 1000 |
| ECI | 0111 |

FIG. 5

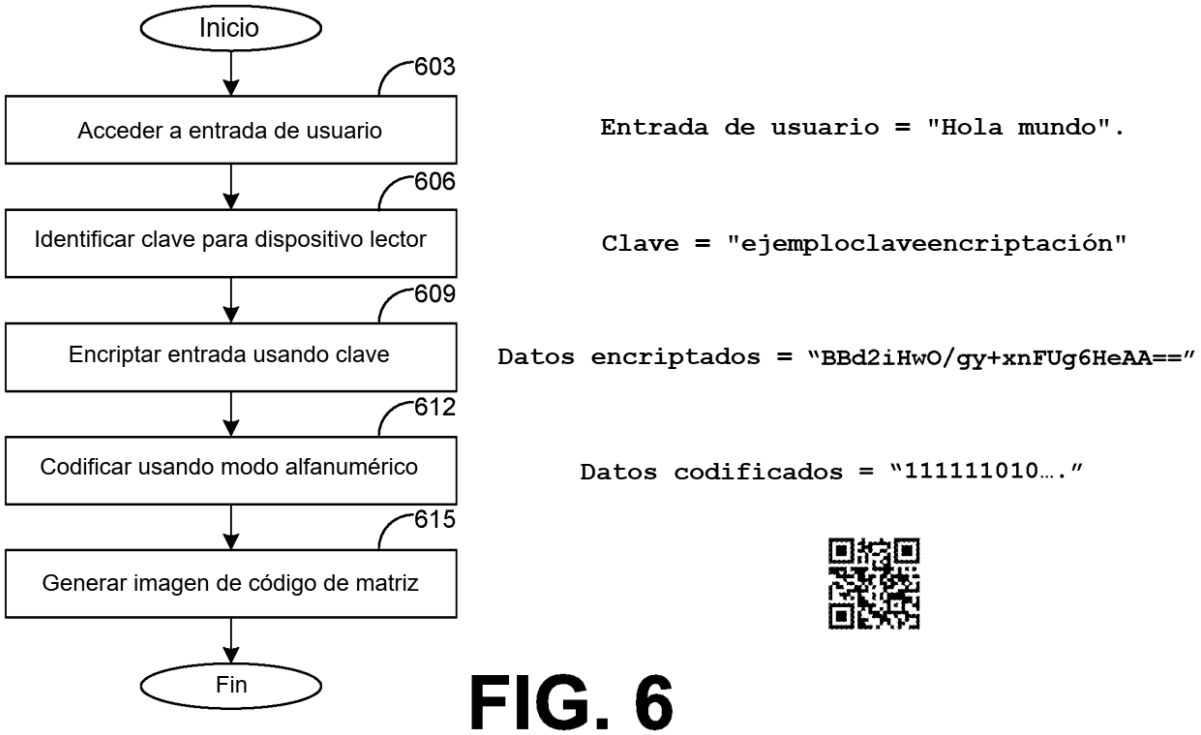


FIG. 6

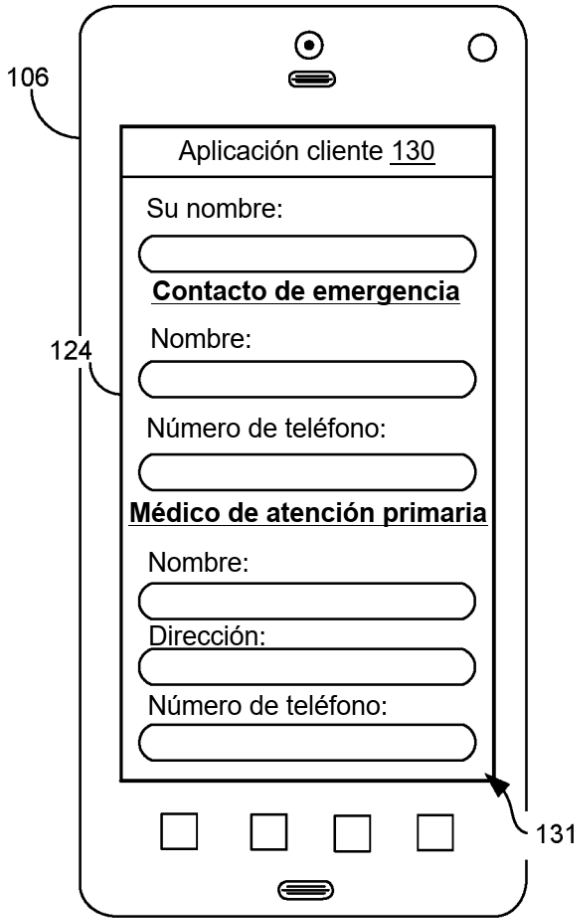
106
Aplicación cliente 130
Su nombre:
Contacto de emergencia
124
Nombre:
Número de teléfono:
Médico de atención primaria
Nombre:
Dirección:
Número de teléfono:
131

FIG. 7A

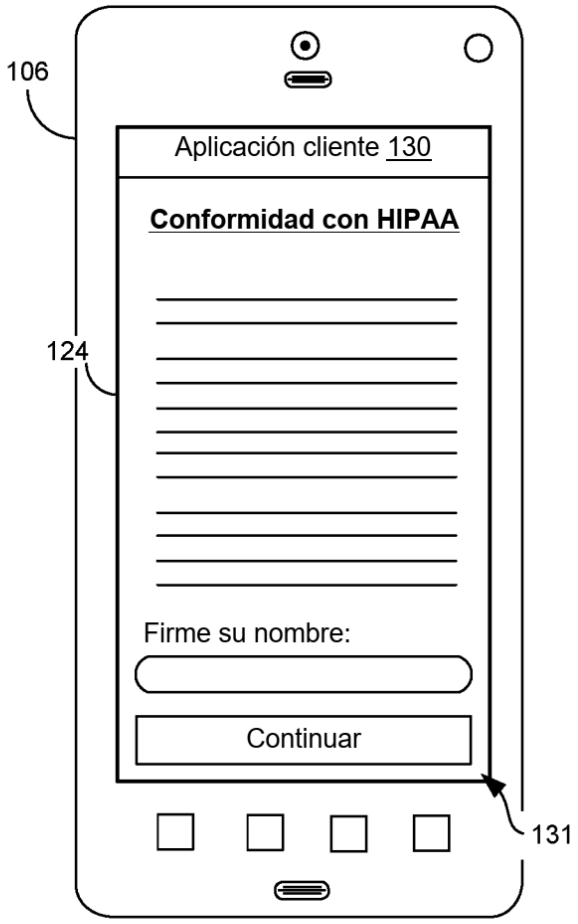
106
Aplicación cliente 130
Conformidad con HIPAA
124
Firme su nombre:
Continuar
131

FIG. 7B

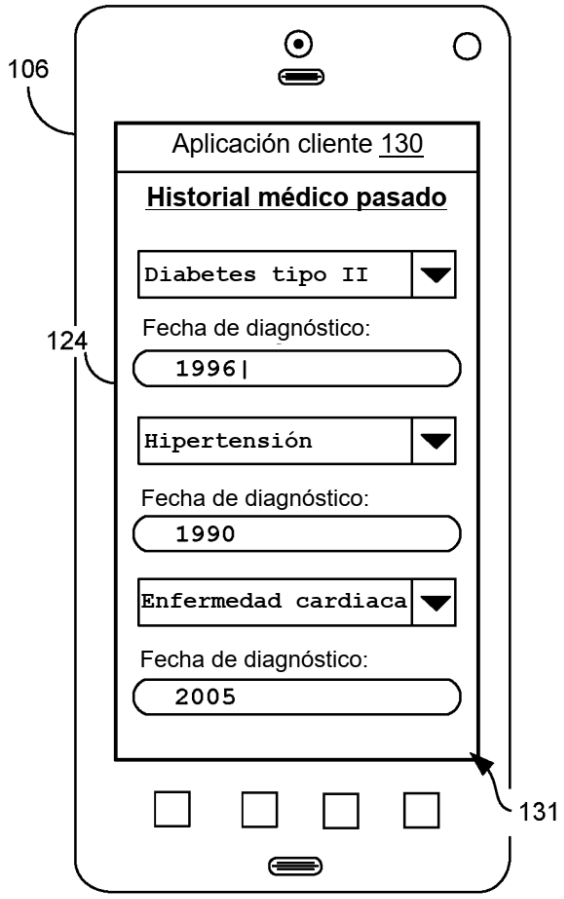
106
Aplicación cliente 130
Historial médico pasado
Diabetes tipo II
124
Fecha de diagnóstico:
1996|
Hipertensión
Fecha de diagnóstico:
1990
Enfermedad cardiaca
Fecha de diagnóstico:
2005
131

FIG. 7C

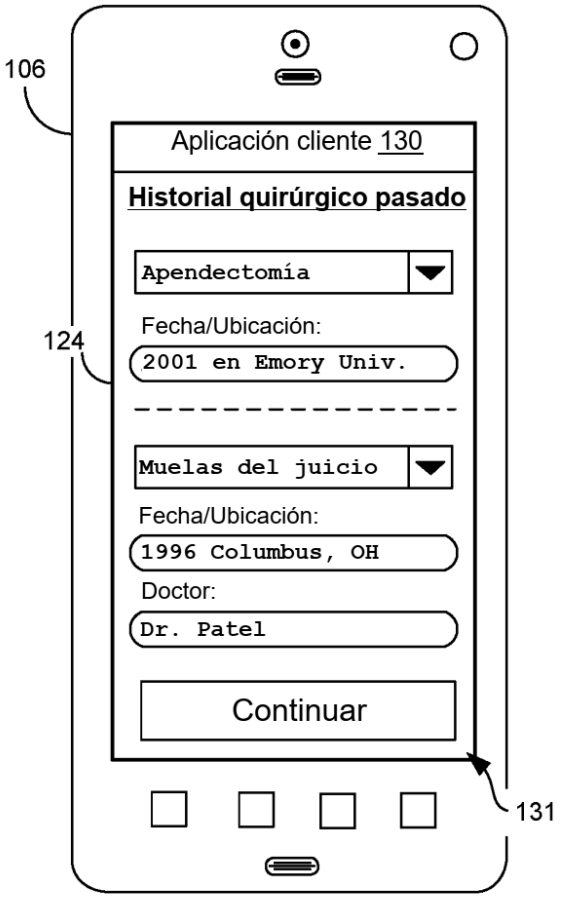
106
Aplicación cliente 130
Historial quirúrgico pasado
Apendectomía
124
Fecha/Ubicación:
2001 en Emory Univ.
Muelas del juicio
Fecha/Ubicación:
1996 Columbus, OH
Doctor:
Dr. Patel
Continuar
131

FIG. 7D

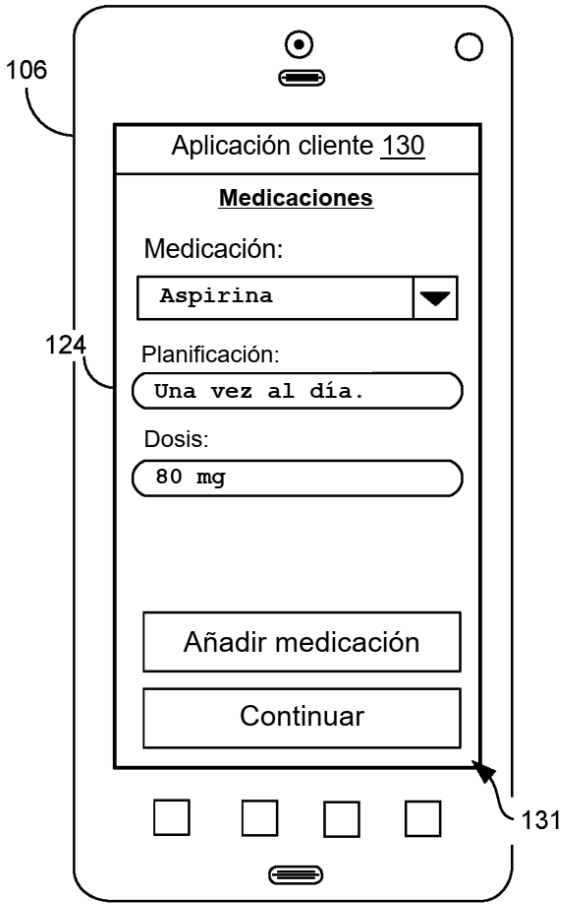
106
Aplicación cliente 130
Medicaciones
Medicación:
Aspirina
124
Planificación:
Una vez al día.
Dosis:
80 mg
Añadir medicación
Continuar
131

FIG. 7E

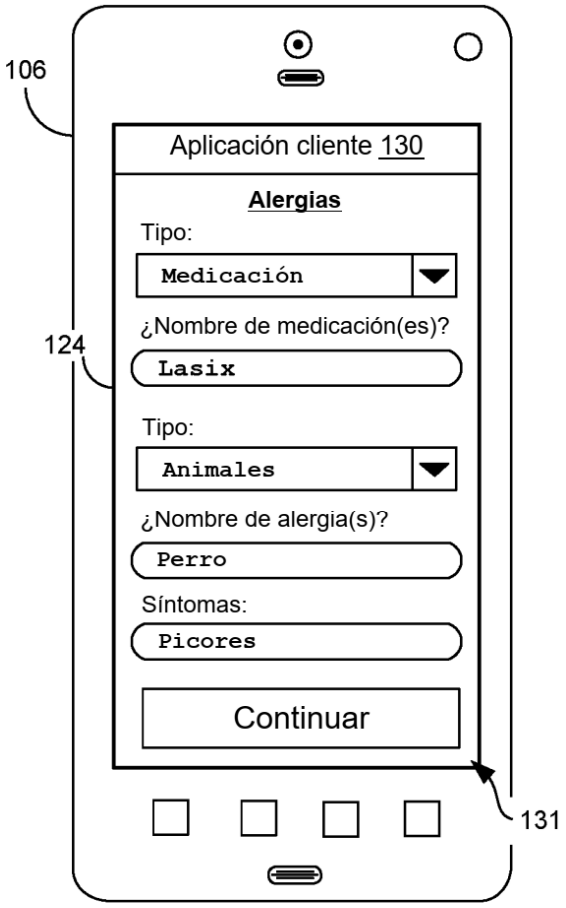
106
Aplicación cliente 130
Alergias
Tipo:
Medicación
124
¿Nombre de medicación(es)?
Lasix
Tipo:
Animales
¿Nombre de alergia(s)?
Perro
Síntomas:
Picores
Continuar
131

FIG. 7F

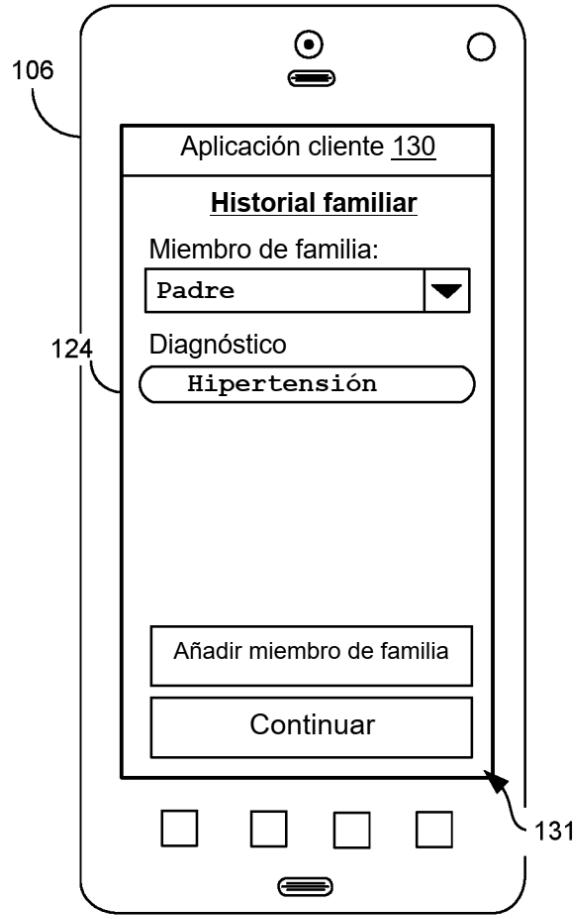
106
Aplicación cliente 130
Historial familiar
Miembro de familia:
Padre
124
Diagnóstico
Hipertensión
Añadir miembro de familia
Continuar
131

FIG. 7G

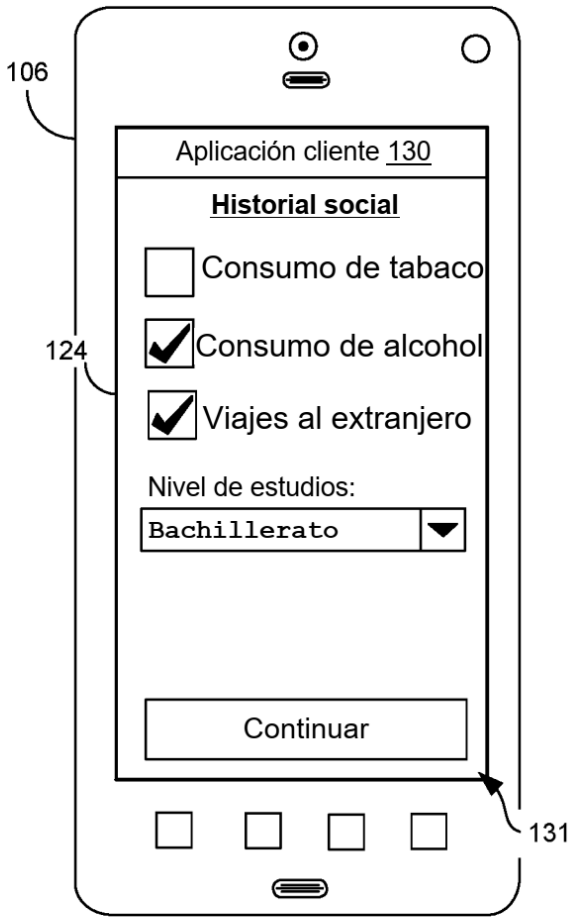
106
Aplicación cliente 130
Historial social
Consumo de tabaco
124
Consumo de alcohol
Viajes al extranjero
Nivel de estudios:
Bachillerato
Continuar
131

FIG. 7H

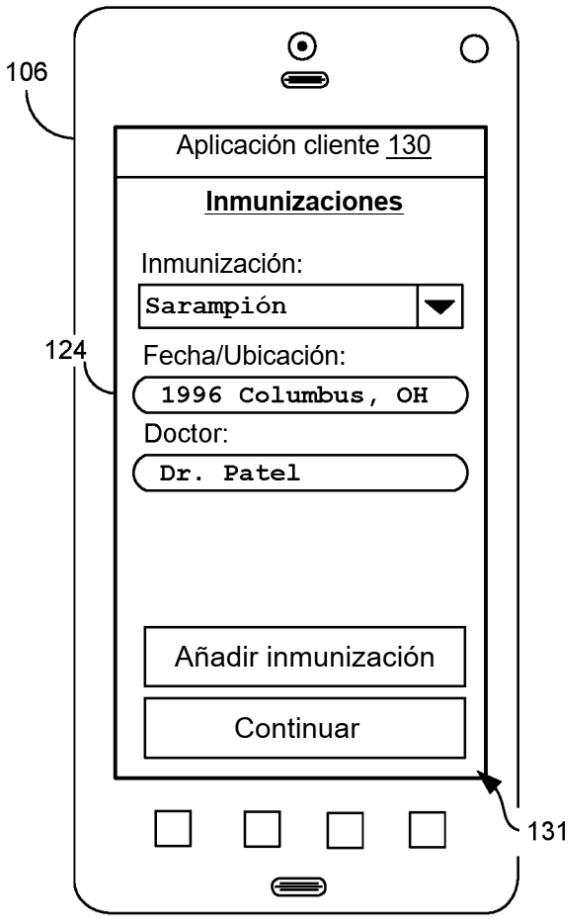
106
Aplicación cliente 130
Inmunizaciones
Inmunización:
Sarampión
124
Fecha/Ubicación:
1996 Columbus, OH
Doctor:
Dr. Patel
Añadir inmunización
Continuar
131

FIG. 7I

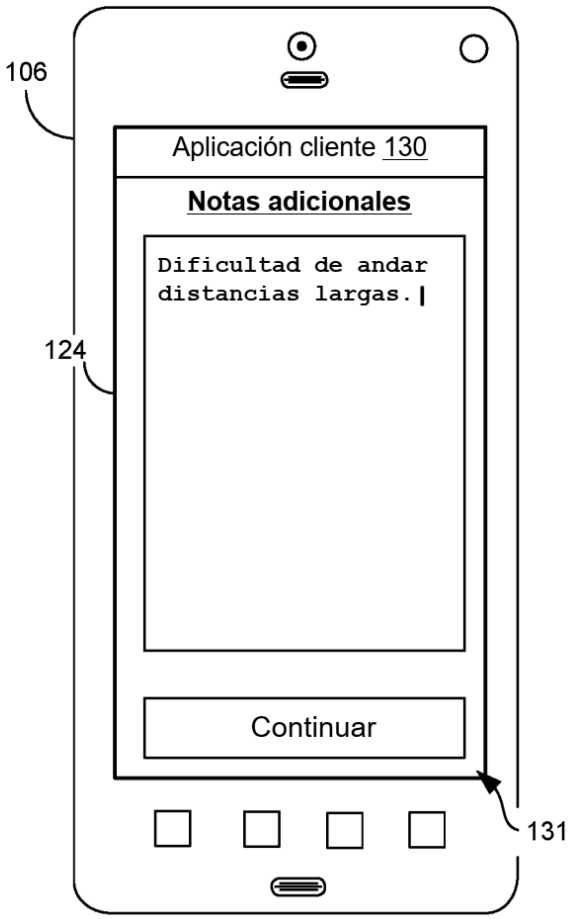
106
Aplicación cliente 130
Notas adicionales
Dificultad de andar distancias largas.
124
Continuar
131

FIG. 7J

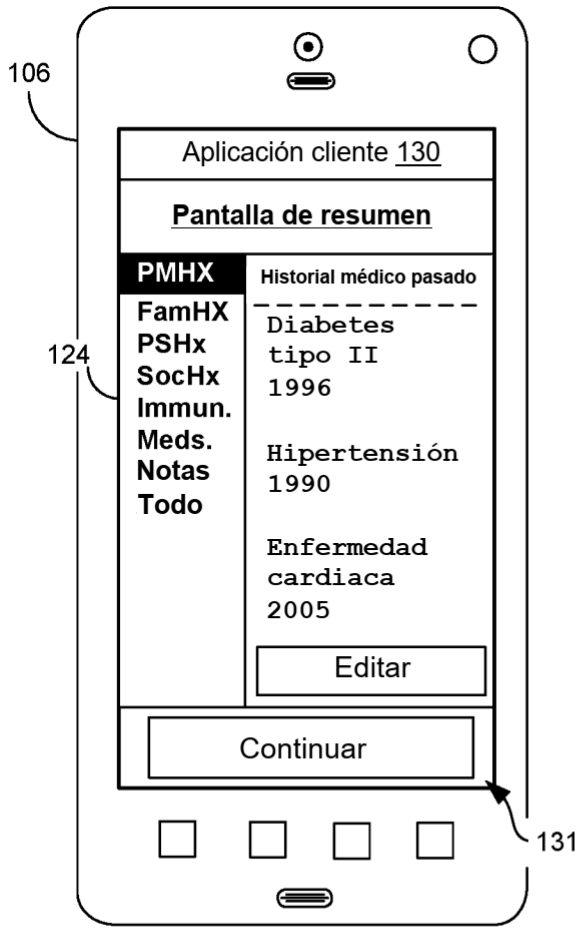
106
Aplicación cliente 130
Pantalla de resumen
PMHX
FamHX
PSHx
SocHx
Immun.
Meds.
Notas
Todo
124
Historial médico pasado
Diabetes tipo II 1996
Hipertensión 1990
Enfermedad cardiaca 2005
Editar
Continuar
131

FIG. 7K

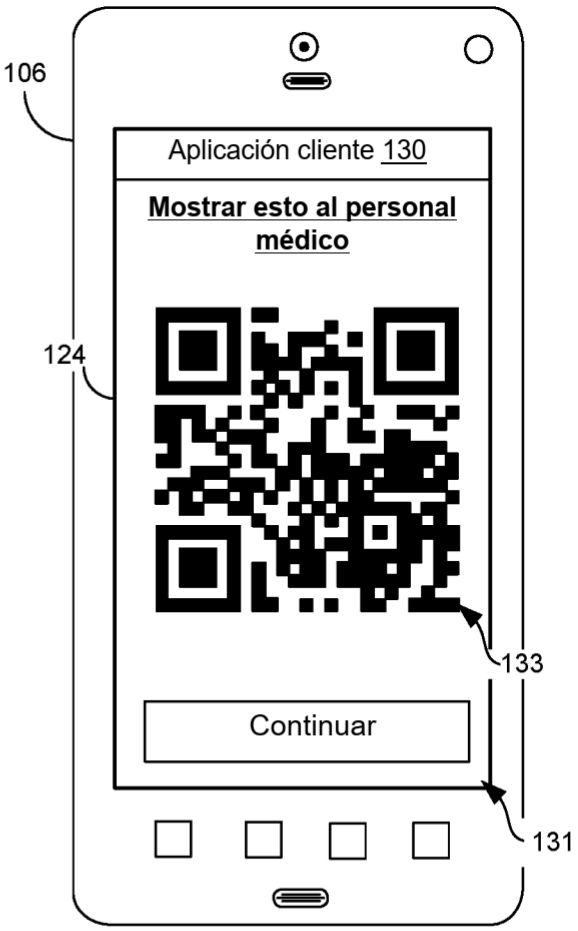
106
Aplicación cliente 130
Mostrar esto al personal médico
124
133
Continuar
131

FIG. 7L

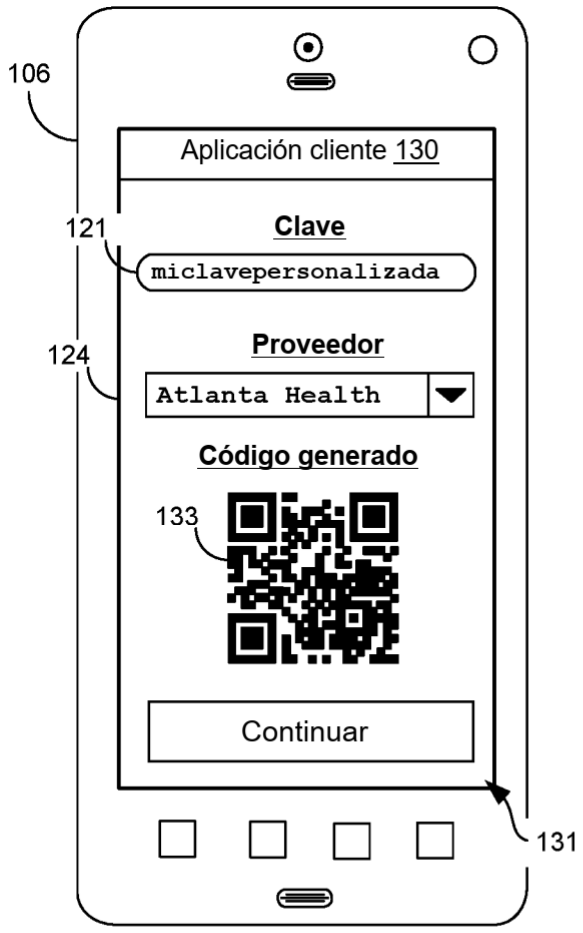
106
Aplicación cliente 130
121
Clave
miclavepersonalizada
124
Proveedor
Atlanta Health
Código generado
133
Continuar
131

FIG. 7M

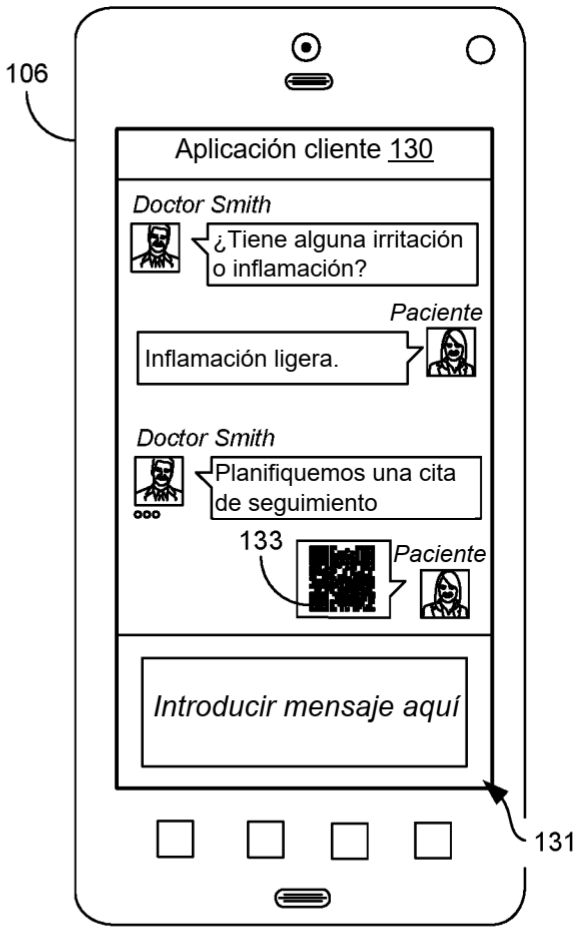
106
Aplicación cliente 130
Doctor Smith
¿Tiene alguna irritación o inflamación?
Paciente
Inflamación ligera.
Doctor Smith
Planifiquemos una cita de seguimiento
133
Paciente
Introducir mensaje aquí
131

FIG. 7N

```
01    func generateMatrixCode() {
02          payloadData = getInputData();    // Conseguir entrada de usuario de UI
03          key = getKey(receiverDevice);    // Conseguir clave para dispositivo receptor
04          modeIndicator = "0010";          // Modo alfanumérico
05          charCount = sizeOf(payloadData); // Conseguir tamaño de caracteres de datos de carga útil
06          encryptedData = encrypt(payloadData, key); // Encriptar datos de carga útil
07          error = calculateError(encryptedData);     // Código de error de Reed Solomon
08          a = formatData(modeIndicator, charCount,
09                         encryptedData, error);      // Datos de formato
10          return generateMatrixImage(a);             // Imagen de código de matriz
11    }
```

800

FIG. 8

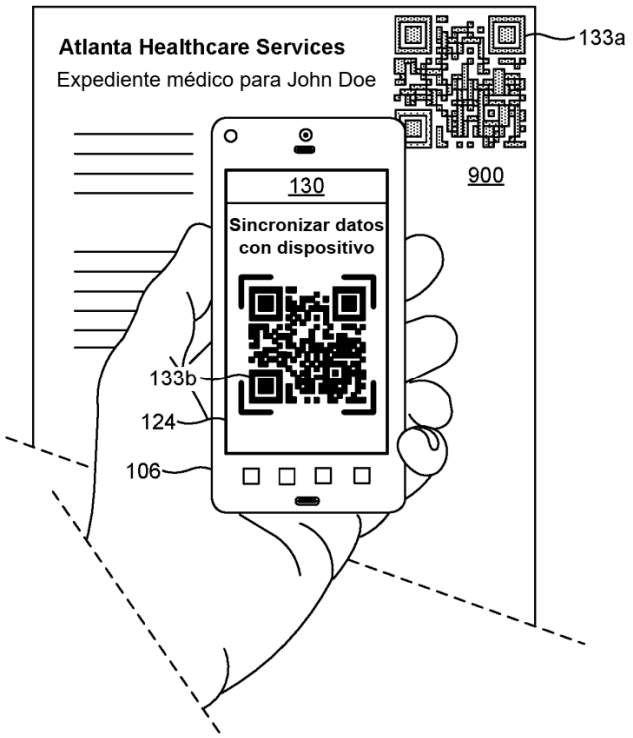


FIG. 9

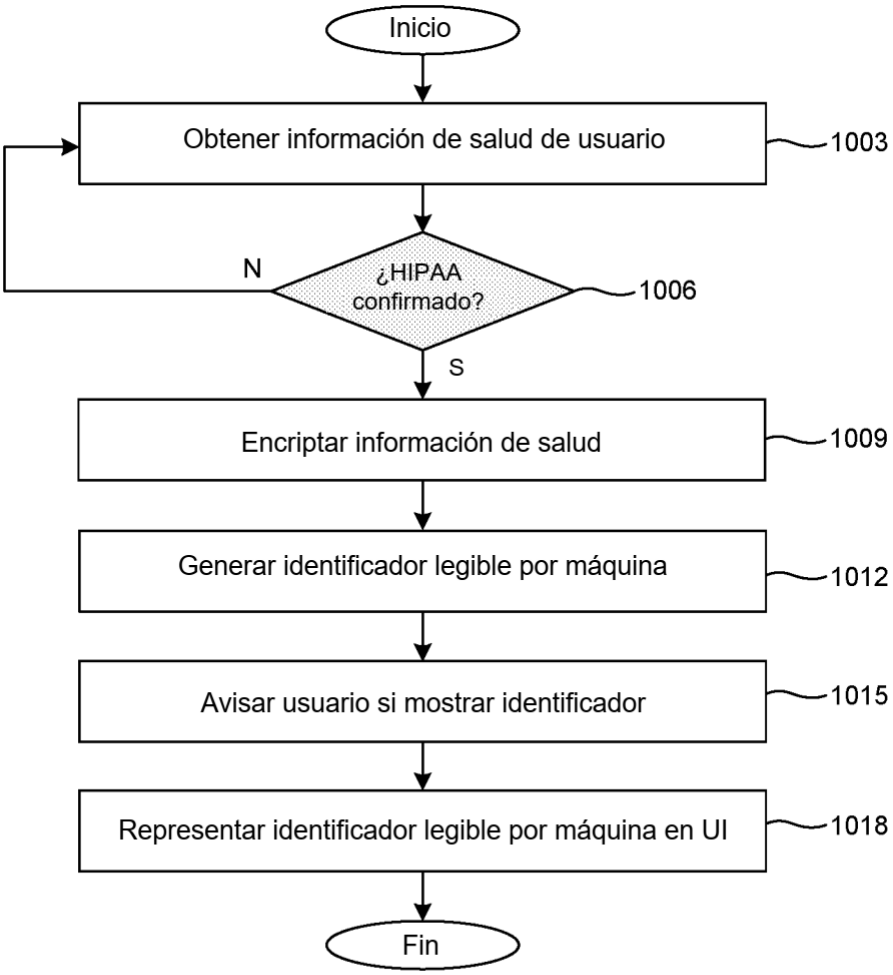
Inicio
Obtener información de salud de usuario
1003
¿HIPAA confirmado?
1006
N
S
Encriptar información de salud
1009
Generar identificador legible por máquina
1012
Avisar usuario si mostrar identificador
1015
Representar identificador legible por máquina en UI
1018
Fin

FIG. 10

130

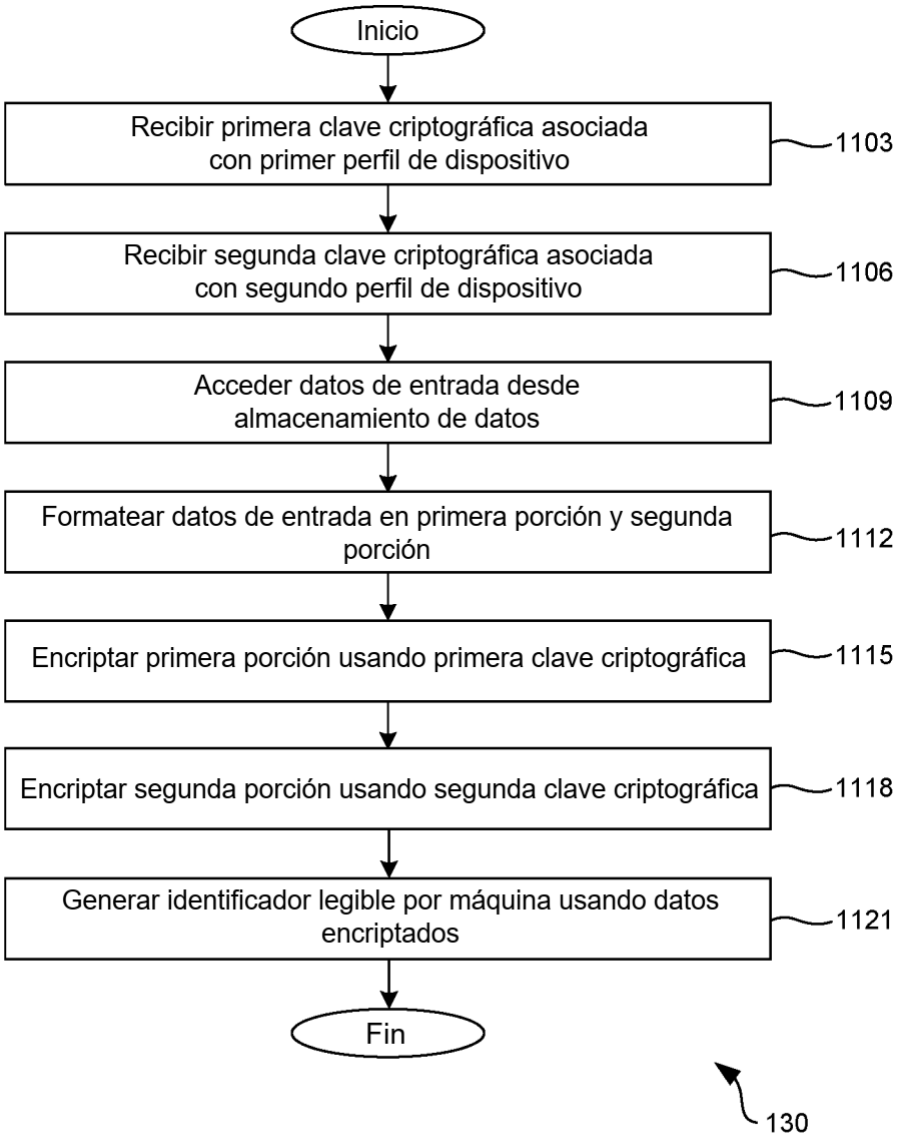
Inicio
Recibir primera clave criptográfica asociada con primer perfil de dispositivo
1103
Recibir segunda clave criptográfica asociada con segundo perfil de dispositivo
1106
Acceder datos de entrada desde almacenamiento de datos
1109
Formatear datos de entrada en primera porción y segunda porción
1112
Encriptar primera porción usando primera clave criptográfica
1115
Encriptar segunda porción usando segunda clave criptográfica
1118
Generar identificador legible por máquina usando datos encriptados
1121
Fin
130

FIG. 11

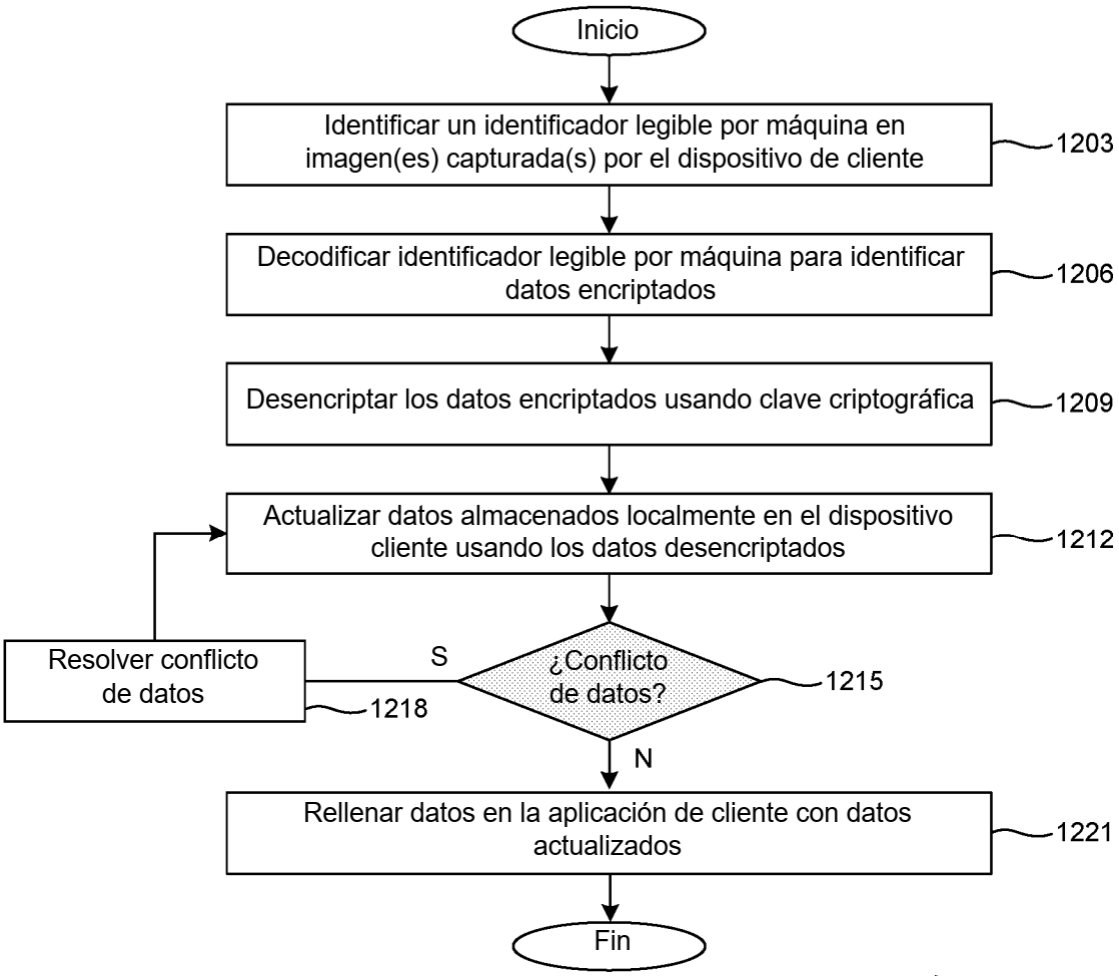
Inicio
Identificar un identificador legible por máquina en imagen(es) capturada(s) por el dispositivo de cliente
1203
Decodificar identificador legible por máquina para identificar datos encriptados
1206
Desencriptar los datos encriptados usando clave criptográfica
1209
Actualizar datos almacenados localmente en el dispositivo cliente usando los datos desencriptados
1212
¿Conflicto de datos?
1215
S
Resolver conflicto de datos
1218
N
Rellenar datos en la aplicación de cliente con datos actualizados
1221
Fin
130

FIG. 12

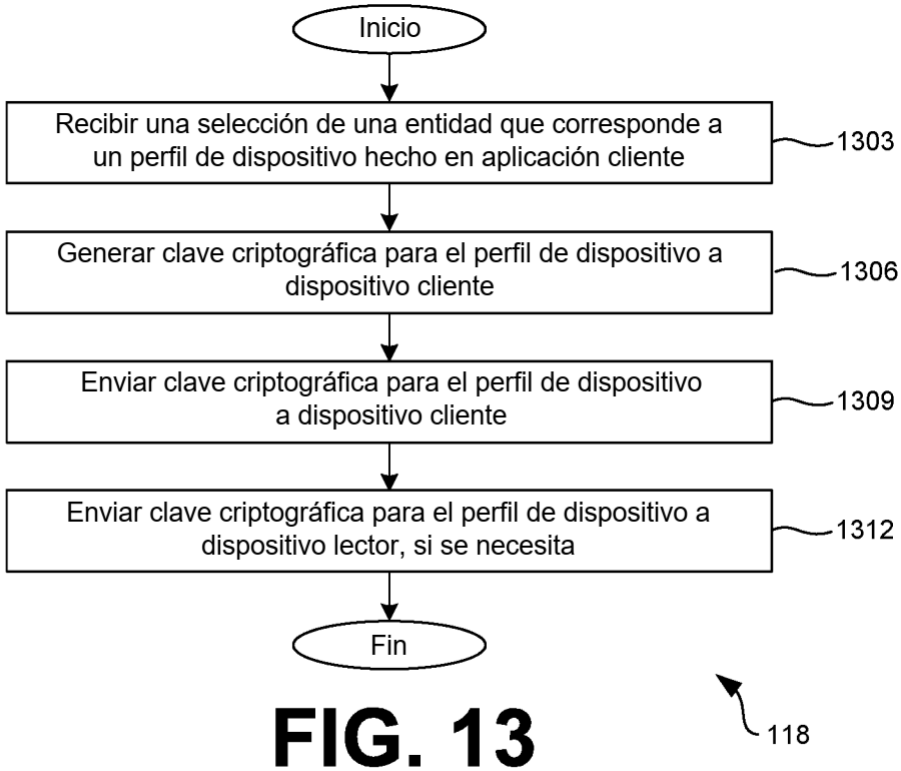
Inicio
Recibir una selección de una entidad que corresponde a un perfil de dispositivo hecho en aplicación cliente
1303
Generar clave criptográfica para el perfil de dispositivo a dispositivo cliente
1306
Enviar clave criptográfica para el perfil de dispositivo a dispositivo cliente
1309
Enviar clave criptográfica para el perfil de dispositivo a dispositivo lector, si se necesita
1312
Fin
118

FIG. 13

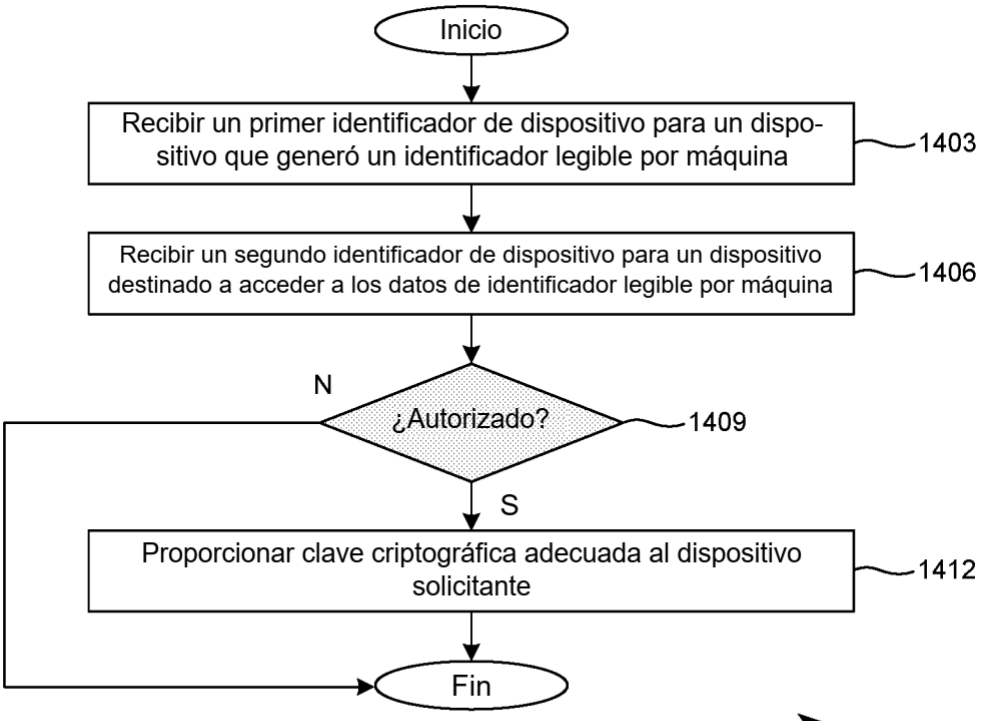
Inicio
Recibir un primer identificador de dispositivo para un dispositivo que generó un identificador legible por máquina
1403
Recibir un segundo identificador de dispositivo para un dispositivo destinado a acceder a los datos de identificador legible por máquina
1406
N
¿Autorizado?
1409
S
Proporcionar clave criptográfica adecuada al dispositivo solicitante
1412
Fin
118

FIG. 14

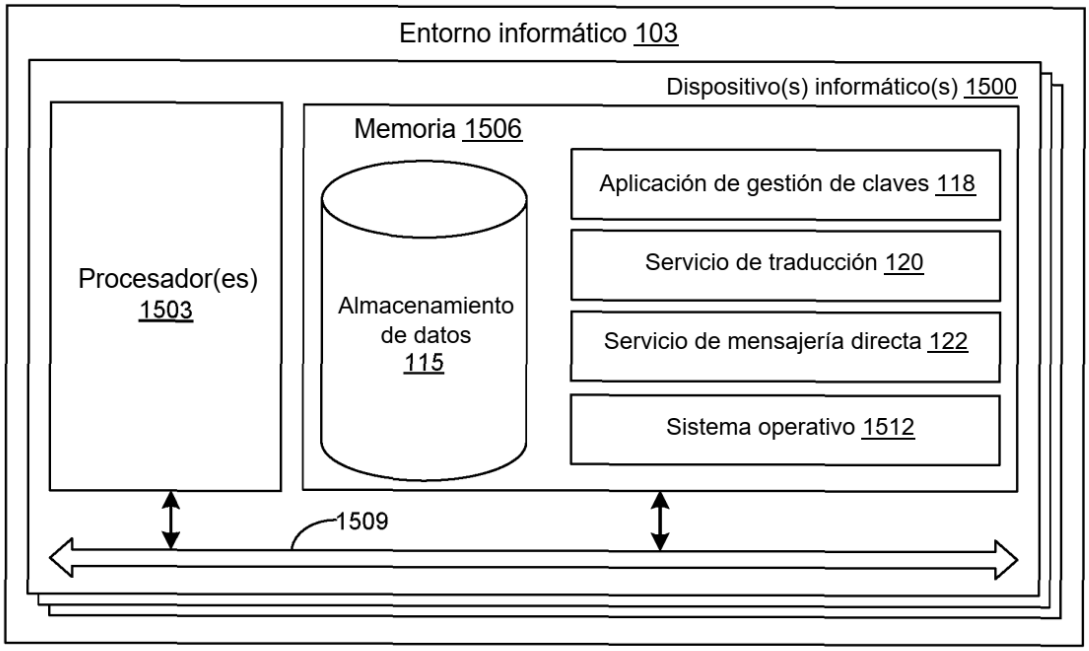


FIG. 15

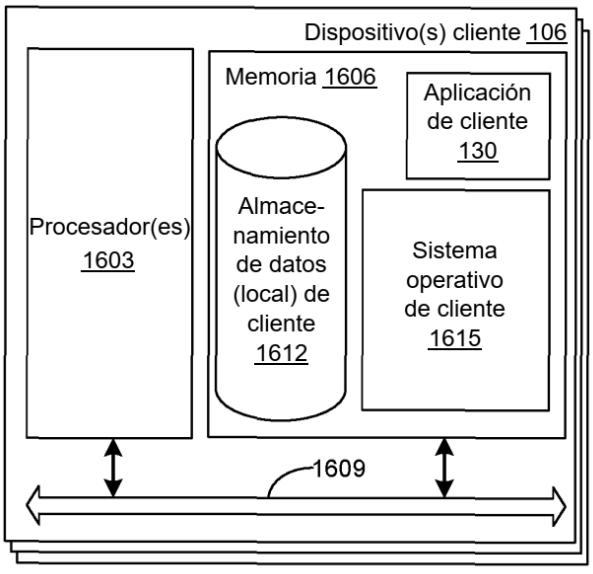


FIG. 16

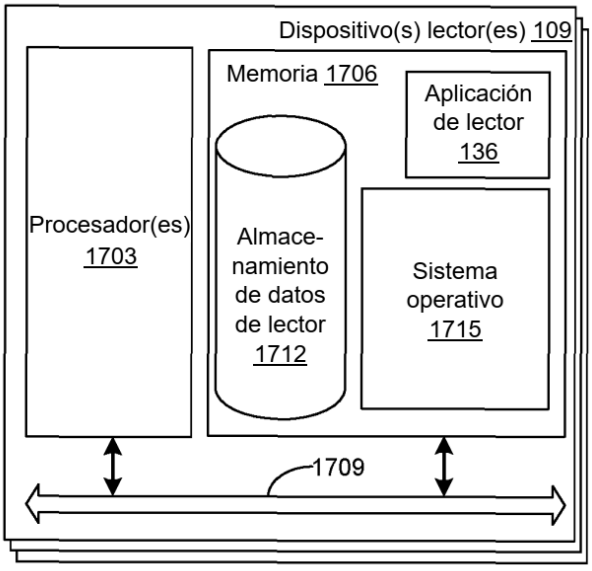


FIG. 17