(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 150**

(51) Int. CI.:

G06F 19/00 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.07.2012 PCT/CA2012/000648**

(87) Fecha y número de publicación internacional: **10.01.2013 WO13003949**

(96) Fecha de presentación y número de la solicitud europea: **05.07.2012 E 12808070 (2)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2729913**

(54) Título: **Métodos para acceder de forma remota a registros médicos electrónicos sin autorización previa**

(30) Prioridad:

05.07.2011 US 201161504526 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2018

(73) Titular/es:

HIPAAT INC. (100.0%)
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, CA

(72) Inventor/es:

CALLAHAN, TERRANCE;
BIALACH, ROMAN y
YEUNG, CHUN MAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Métodos para acceder de forma remota a registros médicos electrónicos sin autorización previa

Campo de la invención

La presente invención se refiere al acceso a información personal de salud (PHI), registros electrónicos de salud (EHR) o registros médicos electrónicos (EMR) y, más específicamente, a métodos y a sistemas para acceder de forma remota a la información personal electrónica de salud del paciente sin autorización previa y/o autentificación.

Antecedentes de la invención

El paso a los registros de salud electrónicos sin papel y el acceso en línea a los registros de salud para la información de salud personal (PHI) está comenzando a ganar impulso.

En el entorno actual, sin embargo, el acceso a PHI, particularmente en un formato digital o electrónico (por ejemplo, EHR/EMR), puede ser difícil y fragmentado. Típicamente, copias de datos médicos pueden mantenerse en clínicas individuales, hospitales, laboratorios u otras ubicaciones remotas para el paciente/usuario. Todo lo anterior, sin embargo, debe informarse al médico de atención primaria. Esta es la razón por la cual el acceso al EHR/EMR del médico de cabecera u hospital es una fuente única de la PHI más completa. Si un paciente visita más de una clínica, por ejemplo, ese paciente puede tener una pluralidad de EHR/EMR. Por ejemplo, el paciente puede visitar una primera clínica y crear un primer registro médico y el paciente puede visitar posteriormente una segunda clínica y crear un segundo registro médico. Si la segunda clínica no tiene acceso al primer EHR/EMR, el examen y el diagnóstico en la segunda clínica pueden ser duplicados e ineficientes. Una actualización de EHR/EMR individuales no garantiza que cada copia se actualice. En consecuencia, la información del registro médico del paciente difiere según la entidad. En consecuencia, es difícil ubicar un registro médico completamente actualizado, y es posible que un médico tratante no pueda obtener una imagen completa de la salud de un paciente antes del tratamiento.

Además, esta naturaleza descentralizada de los EHR/EMR del paciente típicamente no permite que un paciente revise un informe completo de su historial médico y diversas afecciones. El paciente puede no tener la capacidad de acceder o actualizar sus registros médicos. Además, es posible que el paciente no tenga la capacidad de restringir el acceso a sus registros médicos.

Existen situaciones, como las que pueden producirse en una emergencia médica, en las que un proveedor de atención médica puede necesitar acceso a la PHI de un paciente en particular. Esto es particularmente cierto cuando un paciente está fuera de su localidad y puede no tener acceso directo o indirecto a su conjunto de registros médicos (por ejemplo, el paciente está viajando). Si existe un requisito de tratamiento médico u otros proveedores de servicios médicos, puede ser difícil obtener acceso a la PHI del EHR/EMR pertinente. El problema de controlar, autorizar y autentificar el acceso a los HCE/RCE relevantes presenta desafíos significativos. Los administradores del sistema EHR/EMR pueden permitir que ciertos proveedores accedan a la PHI de un paciente usando una contraseña/frase clave. Los administradores actuales de EHR/EMR requieren que se autorice previamente a los proveedores de atención médica para ver la PHI de un paciente en el EHR o EMR. Comúnmente, es posible que no haya forma de que un proveedor de atención médica acceda a la PHI relevante sin la previa autorización del administrador de EHR/EMR. Las publicaciones de patente US 6 073 106 A y US 2011/022414 A1 describen información que es útil para comprender los antecedentes de la invención.

Por lo tanto, es necesario que un sistema permita que los proveedores de atención médica y otros tengan acceso remoto inmediato a la PHI de un paciente sin que el anterior tenga conocimiento previo de quién es el proveedor y sin comprometer la privacidad y la seguridad de la información de salud personal del paciente. Además, existe la necesidad de acceder a la PHI de un paciente particular que resida en una pluralidad de sistemas EHR/EMR no relacionados.

Sumario de la invención

Por consiguiente, la presente invención se dirige a un método para permitir que un usuario remoto tenga acceso a un registro médico electrónico de un paciente de acuerdo con las reivindicaciones adjuntas.

En una realización adicional de la divulgación, el protocolo de autorización específica del paciente se basa en criterios de autorización del paciente predeterminados.

En aún una realización adicional de la divulgación, los criterios de autorización del paciente se determinan antes de la etapa (a) anterior.

En aún una realización adicional de la divulgación, los criterios de autorización del paciente predeterminados son un número de identificación específico del paciente y una frase de contraseña específica del paciente.

En aún otra realización adicional de la divulgación, el protocolo de consentimiento específico del paciente se basa en criterios de consentimiento del paciente predeterminados.

En aún una realización adicional de la divulgación, los criterios de consentimiento del paciente predeterminados se determinan por el paciente antes de la etapa (a).

En aún una realización adicional de la divulgación, los criterios de consentimiento del paciente predeterminados se determinan a partir de una política de consentimiento específica del paciente.

En aún una realización adicional de la divulgación, el método comprende además la etapa de proporcionar al menos una parte de información de usuario remoto al segundo equipo en la etapa (a) y la etapa de la tercera red informática que se comunica con una cuarta red informática para identificar al usuario remoto a través de al menos una parte de la información de usuario remoto y dependiente de un protocolo de identificación del usuario remoto. En otra realización más, la cuarta red informática es un registro maestro de proveedores. En otra realización más, el registro maestro de proveedores es el Registro Nacional de Identificadores de Proveedores de EE. UU. o uno de los Registros del Colegio Canadiense de Médicos y Cirujanos.

En aún una realización adicional de la divulgación, el protocolo de identificación de usuario remoto se basa en al menos un criterio de identificación de usuario predeterminado.

En aún una realización adicional de la divulgación, la al menos una parte de información de usuario remoto se determina antes de la etapa (a).

En aún una realización adicional de la divulgación, la al menos una parte de información de usuario remoto se selecciona del grupo que consiste de un número de identificación del usuario, un nombre del usuario y una ubicación del usuario.

Breve descripción de los dibujos

Los anteriores y otros objetos, características, y ventajas de la presente invención serán evidentes a partir de la siguiente descripción detallada cuando se toma en conjunción con los dibujos adjuntos.

La figura 1 es una vista de una realización de la presente invención dirigida a componentes del sistema remoto de acceso de emergencia;

La figura 2 es una vista de una realización de la presente invención dirigida a un ordenador del proveedor de atención médica;

La figura 3 es un diagrama de flujo que ilustra esquemáticamente un método para acceso remoto, de acuerdo con una realización de la presente invención;

La figura 4 es una vista de una realización de la presente invención que ilustra la selección inicial por un usuario remoto (por ejemplo, un proveedor remoto);

La figura 5 es una vista de una realización de la presente invención dirigida a ingresar información del usuario remoto;

La figura 6 es una vista de una realización de la presente invención dirigida a ingresar información del paciente; y

La figura 7 es una vista de una realización de la presente invención que muestra una pantalla de verificación del paciente.

Descripción de las realizaciones preferidas

La descripción que sigue, y las realizaciones descritas en la misma, se proporciona a modo de ilustración de un ejemplo o ejemplos, de realizaciones particulares de los principios y aspectos de la presente invención. Estos ejemplos se proporcionan con fines de explicación, y no de limitación, de esos principios y de la invención.

Se entenderá por parte de una persona experta en la técnica relevante que en diferentes regiones geográficas y jurisdicciones a estos términos y definiciones que se utilizan en el presente documento se les pueden dar diferentes nombres, pero se refieren a los mismos sistemas respectivos.

Aunque la presente memoria descriptiva describe componentes y funciones implementadas en las realizaciones con referencia a normas y protocolos conocidos para una persona experta en la técnica, la presente divulgación, así como las realizaciones de la presente invención no se limitan a ningún estándar específico o protocolo. Cada uno de los estándares para Internet y otras formas de transmisión de red informática (por ejemplo, TCP/IP, UDP/IP, HTML y HTTP) representan ejemplos del estado de la técnica. Tales estándares son reemplazados periódicamente por equivalentes más rápidos o más eficientes que tienen esencialmente las mismas funciones. Por consiguiente, los estándares y protocolos de reemplazo que tienen las mismas funciones se consideran equivalentes.

En la siguiente memoria descriptiva, los términos "información personal de salud", "información de salud del paciente" "información médica protegida" o "PHI" se usan indistintamente y se entenderá por parte de una persona

experta en la técnica que significa información de salud acerca o relacionada con un paciente, que incluye, entre otros, información relacionada con uno o más de los siguientes: (a) la salud física o mental de la persona, incluida la información que consiste en el historial de salud de la familia de la persona; (b) la provisión de atención médica a la persona, incluida la identificación de una persona como proveedor de atención médica para la persona; (c) se relaciona con pagos o elegibilidad para atención médica, o elegibilidad para cobertura de atención médica, con respecto a la persona; y (d) un número de identificación del paciente.

En la siguiente memoria descriptiva, los términos "acceso remoto" y similares se comprenderán por parte de una persona experta en la técnica relevante que se refieren a que tiene acceso desde un ordenador, una red o sistema remoto de (por ejemplo, cualquier distancia de) la ubicación de otro sistema (por ejemplo, un sistema EHR/EMR) mediante el cual los dos sistemas se comunican a través de un enlace de datos (por ejemplo, una red), que puede ser seguro. El acceso remoto está disponible por cualquier número de enlaces de datos seguros, como, por ejemplo, una red interna (intranet), un proveedor de servicios de Internet (ISP), conexión de acceso telefónico a través de escritorio, ordenador portátil o módem portátil a través de la línea telefónica regular, o una línea dedicada entre un ordenador o una red de área local remota y la red de área local principal o "central". El acceso remoto también se puede usar como parte de una red privada virtual (VPN). Una persona experta en la técnica relevante entenderá además que un "usuario remoto" es un usuario que tiene acceso remoto.

En la siguiente memoria descriptiva, los términos "registros electrónicos de salud" o "EHR" se entenderán por parte de una persona experta en la técnica que se refieren a una colección de PHI en formato electrónico o digital que es capaz de ser compartida a través de diferentes sistemas de información de atención médica, a través del sistema de información de toda la empresa conectado a la red y otras redes de información o intercambios. Los EHR proporcionan una variedad de datos, que incluyen, entre otros, datos demográficos, historial médico, medicamentos y alergias, estado de vacunación, resultados de pruebas de laboratorio, imágenes de radiología, signos vitales, estadísticas personales como edad y peso e información de facturación.

En la siguiente memoria descriptiva, los términos "registros médicos electrónicos" o "EMR" se entenderán por parte de una persona experta en la técnica en el sentido de un registro médico electrónico o digital creado o grabado en una organización (por ejemplo, hospital, clínica, proveedor de seguros, etc.) que contiene EHR.

En la siguiente memoria descriptiva, los términos "registro de proveedor maestro" o "MPR" se entenderán por parte de una persona experta en la técnica que se refiere a cualquier registro o directorio que proporciona información de profesionales de la salud dentro de una jurisdicción específica y se utiliza en la industria de la salud para proporcionar presentaciones electrónicas de documentos según las leyes y regulaciones aplicables.

La invención comprende ampliamente un método y un sistema para permitir que los pacientes, los profesionales de la salud y otros, incluyendo proveedores de servicios, para tener acceso remoto a la PHI de un paciente a través de acceso remoto a los EHR y/o EMR. Las realizaciones de la presente invención proporcionan sistemas y métodos para proporcionar servicios de salud digitales personalizados e interconectados.

Hay situaciones, como puede ocurrir en una emergencia médica, donde un profesional de la salud puede tener acceso a la PHI de un paciente en particular sin haber tenido una relación previa con el paciente y, por lo tanto, la política de acceso a la información proveedor/paciente no será conocido por los sistemas aplicables que autentifican y/o autorizan el acceso a la PHI del paciente. En otras palabras, puede ser necesario en tales circunstancias que un usuario (por ejemplo, un proveedor de atención médica) requiera acceso al EHR/EMR aplicable sin autorización previa y/o autentificación previa por parte del paciente u otras personas. Esto es particularmente cierto cuando un paciente está fuera de su localidad y puede no tener acceso directo o indirecto a su conjunto de registros médicos (por ejemplo, el paciente está viajando). Si existe un requisito de tratamiento médico u otros proveedores de servicios médicos, puede ser difícil acceder a estos registros médicos electrónicos.

La presente invención se dirige a un servicio remoto de registro médico electrónico de acceso (REMRAS) y/o a un sistema que está conectado operativamente a las redes o sistemas aplicables (por ejemplo, sistemas de EHR o EMR, CVS, MPR, servicios de identificación/autentificación de proveedores, etc.) Los sistemas EHR o EMR son bien conocidos por una persona experta en la técnica y típicamente comprenden un sistema en línea que contiene el EHR/EMR relevante de un paciente. El REMRAS de la presente invención también puede estar conectado operativamente a servicios de identificación de proveedores, tales como un registro maestro de proveedores (MPR), que puede comprender una fuente central y autorizada de proveedores o profesionales de la salud enumerados, incluyendo dónde trabajan y cómo ser contactados, generalmente un sistema en línea, que también se puede utilizar para proporcionar información sobre los usuarios. El REMRAS de la presente invención también puede estar conectado operativamente a servicios de autentificación de proveedores, tales como Equifax/Anakam, Auththentify o Resilient Networks, que pueden comprender una fuente central y autorizada de información de proveedores de atención médica que se puede usar para autentificar el usuario o proveedor remoto identificado. Finalmente, el REMRAS de la presente invención también puede estar operativamente conectado a un servicio de gestión y/o validación de consentimiento (CVS) que puede contener además criterios de autorización derivados del paciente.

La figura 1 es un diagrama de bloques de una realización de la presente invención **100** para permitir el acceso remoto a datos del paciente, que incluyen, entre otros, registros electrónicos de salud. La realización de la presente

invención mostrada como se muestra en la figura 1 está constituida por los diversos componentes conectados de manera operativa o unidos de otro modo por medio de una red informática 104, que incluye, pero no se limita a, Internet. Como se muestra en la figura 1, se proporciona un sistema de Registro Médico Electrónico (EMR) **101** que contiene información de salud protegida (PHI) del paciente, tal como será familiar y/o requerido por aquellos que practican o prestan servicios en el campo médico, como, por ejemplo, ejemplo, profesionales/proveedores de salud y proveedores de seguros. Como se muestra en la figura 1, también se proporciona un componente de portal **102** y un componente de servicio de gestión/validación de consentimiento (CVS) **103.** La realización de la realización mostrada que se muestra en la figura 1 también puede incluir un servicio o sistema **107** (por ejemplo, registro principal de proveedores (MPR)) que se comunica a través de la red **104** y una estación de trabajo u ordenador **106**, similar que es utilizada por un proveedor de servicios de salud y está conectada operativamente a la red **104** (por ejemplo, capaz de descargar software, como, por ejemplo, aplicaciones y páginas web de acceso) y un Servicio de Autentificación de Proveedores **105** utilizado para autentificar a un usuario remoto (por ejemplo, un proveedor remoto). Cada uno de estos componentes se analizará en mayor detalle a continuación.

Como se muestra en la figura 2, la estación de trabajo **106** puede comprender el elemento de interfaz **210** y otros elementos funcionales requeridos para la estación de trabajo que un experto en la técnica pertinente entendería, incluidos los de al menos un ordenador de propósito general especialmente programado. Se entenderá que el elemento de interfaz **210** puede comprender una interfaz gráfica de usuario (GUI) como una interfaz hombre-ordenador (es decir, una forma en que los humanos interactúan con los ordenadores) que usa ventanas, iconos y menús que pueden ser manipulados mediante un ratón (y a menudo de forma limitada por un teclado también). El elemento de interfaz es para recibir datos con respecto a al menos una condición ambiental relacionada con el paciente, que incluye, pero no se limita a, al menos un síntoma relacionado con la salud física o mental del paciente y datos de antecedentes del paciente. En una realización preferida, el elemento de interfaz 210 puede comprender un navegador web o un navegador.

La información del usuario remoto (por ejemplo, proveedor de cuidados de salud) se puede utilizar para identificar a un usuario remoto y determinar la identificación, la autentificación y/o la autorización. Mediante estas credenciales aplicables del proveedor de atención médica y la posterior identificación, autentificación y/o autorización, los usuarios remotos, incluidos, entre otros, los proveedores remotos, pueden tener acceso al sistema EMR o EHR del paciente. La autorización final de un proveedor remoto para acceder a la PHI en un EMR o EHR también puede requerir el uso de un servicio de validación de consentimiento (CVS).

De acuerdo con la realización de la presente invención, se proporciona un servicio de gestión de consentimiento que permite a los administradores del EMR crear y administrar reglas de divulgación de PHI de privacidad específicas del paciente y una contraseña o frase de contraseña en nombre del paciente. En una realización preferida, se puede informar a un paciente que su PHI es privada y que los proveedores de atención médica/organizaciones de prestación de atención (CDO) la mantendrán en confianza, sujeta a divulgaciones permitidas por las organizaciones que la mantienen. Además, se informa al paciente que estas organizaciones pueden tener obligaciones de privacidad con respecto a la divulgación (intercambio) de la PHI. Según lo resuelto por el CVS, la PHI puede divulgarse con el consentimiento explícito del paciente y solo a través de las prácticas de la presente invención. En una realización preferida, el paciente (o alguien designado) debe proporcionar una información que pueda identificar específicamente a ese paciente (por ejemplo, una frase de contraseña personal). En consecuencia, la divulgación de la PHI puede realizarse a cualquier otra parte que conozca esta frase de contraseña. Si el paciente no puede proporcionar la frase de contraseña aplicable, la divulgación solo se realizará a un proveedor de atención médica autentificado. Además, el paciente puede restringir aún más la divulgación en mayor detalle (por ejemplo, departamentos de emergencia solamente). Estas directivas de consentimiento pueden ser cambiadas posteriormente por el paciente accediendo a un portal específico para el paciente. Una vez que las reglas de acceso han sido creadas a partir de la(s) directiva(s) de consentimiento, un servicio de validación de consentimiento (CVS) aplica estas reglas, adjudicando así la divulgación apropiada de la PHI pertinente.

Al proporcionar el número de identificación del paciente y la frase de contraseña secreta conocida solo por el paciente (y su designado), el paciente está autorizando personalmente y autentificando a cualquier persona que él/ella elige en todo el mundo para tener acceso a la PHI del paciente, sin tener en cuenta de quién o dónde se encuentra la persona. Si el paciente no recuerda su frase de contraseña, o no puede (por ejemplo, está inconsciente) proporcionar su frase de contraseña, entonces el acceso a la PHI puede otorgarse a través de un servicio externo certificado previamente (que puede estar disponible donde se encuentre en ese momento) que autentifica a la persona como ese usuario remoto específico (por ejemplo, proveedor de atención médica).

En una realización preferida, el paciente puede también predeterminar el departamento(s) (por ejemplo, solo el servicio de urgencias), Estado(s)/Provincia(s) y Países los que cualquier usuario remoto debe estar para tener acceso. Esto se logra al elegir actualizar la política de consentimiento del paciente. Posteriormente, si alguno de estos atributos no coincide con las tolerancias en la política de consentimiento derivada del paciente, entonces no se permitirá el acceso al usuario remoto. En el caso de situaciones en las que no pueda proporcionar su frase de contraseña, y en caso de que el servicio de autentificación del proveedor **105** (por ejemplo, Equifax/Anakam, Auththentify, Resilient Networks, etc.) no pueda autentificar al proveedor de atención médica, se recomienda que el paciente de su frase de contraseña a un contacto de emergencia designado en el dorso de la tarjeta de la billetera del paciente para ser contactado.

En una realización alternativa, el acceso al EMR puede proporcionarse usando un grupo de credenciales. Las credenciales del EMR se pueden aprovisionar específicamente para este fin, de modo que varias cuentas de inicio de sesión diferentes estén disponibles para su uso. Por lo tanto, cada vez que se proporciona acceso a un nuevo proveedor de atención médica, se puede usar una cuenta de usuario de EMR diferente. Esto puede permitir que el EMR registre correctamente las acciones del proveedor y permite que el portal REMRAS **102** elimine la ambigüedad de un proveedor de las acciones de otro proveedor que acceda al EMR en condiciones similares.

En una realización preferida, una vez se ha accedido al portal web, un proveedor puede ser identificado, autentificado, y/o autorizado. En redes informáticas, tales como, por ejemplo, Internet **104,** estas etapas se realizan comúnmente mediante el uso de información derivada del usuario remoto y/o del paciente. En una realización preferida, se asume que el conocimiento de la frase de contraseña derivada del paciente por parte del usuario remoto garantiza que el usuario es auténtico y está autorizado.

Para la identificación y/o con fines de autentificación, cada usuario (por ejemplo, un proveedor de cuidado de la salud) registra inicialmente (o se ha registrado por otra persona), utilizando la información específica del usuario (por ejemplo, una contraseña asignada o autodeclarada). En cada uso posterior, el usuario remoto debe conocer y utilizar la información específica del usuario identificada previamente. Los proveedores de atención médica generalmente deben registrarse, y por lo tanto conocerse, en cada sistema de registros electrónicos en particular en el que se almacena y mantiene el EHR/EMR. Cuando se requiere una mayor seguridad, las transacciones requieren un proceso de autentificación más estricto. Se considera que el uso de certificados digitales emitidos y verificados por una autoridad de certificación (CA) como parte de una infraestructura de clave pública se convertirá en la forma estándar de realizar la autentificación en Internet. Una vez registrado, cada proveedor de atención médica recibirá credenciales que lo identificará en el sistema EHR/EMR aplicable. Aunque este sistema puede ser seguro, es posible que no permita fácilmente el acceso de cada proveedor de atención médica a cada sistema de registros electrónicos en el que se proporcionan los registros electrónicos de salud EHR/EMR (por ejemplo, sistemas EHR/EMR). Un aspecto de la presente invención es incluir un portal de acceso que proporciona acceso a la PHI de un paciente en una pluralidad de fuentes de datos (es decir, sistemas EHR/EMR aplicables) independientemente de si el proveedor de atención médica ha sido registrado o no con un sistema EHR/EMR específico.

En una realización preferida de la invención, la autentificación puede incluir también la autorización. Como se señaló anteriormente, si el usuario remoto tiene la información necesaria derivada del paciente (es decir, la identificación del paciente y la frase de contraseña), el usuario remoto puede estar autentificado y autorizado.

La figura 3 es un diagrama de flujo que ilustra esquemáticamente el método de acceso remoto descrito en el presente documento de acuerdo con la operación de una realización de la presente invención. El método comienza en **301** donde, como resultado de una ocurrencia médica inesperada, por ejemplo, un accidente en un lugar extranjero, un paciente puede presentarse a un proveedor de atención médica (por ejemplo, el proveedor A), a quien el paciente no ha visto antes. Durante esta consulta, el proveedor A examina al paciente y luego solicita acceso al historial médico del paciente, que puede ubicarse o almacenarse en un sistema EHR/EMR remoto (por ejemplo, el sistema EMR del proveedor de atención médica del paciente). Es posible que se requiera la PHI de este paciente para proporcionar el mejor tratamiento para el paciente. Para proporcionar acceso al proveedor A a la PHI contenida dentro del sistema EMR aplicable, el proveedor A debe obtener los detalles de acceso necesarios o aplicables, normalmente del paciente directamente, para poder interoperar con el sistema EMR aplicable (ver **302**). Un experto en la técnica relevante entenderá que el proveedor A puede contactar con el sistema EMR aplicable a través de cualquier estación de trabajo en red (por ejemplo, la estación de trabajo **106**).

Cuando proveedor A requiere el acceso a la PHI del paciente, él o ella utilizará la interfaz **210** (por ejemplo, un navegador web) en la estación de trabajo en red para acceder a un portal web **102** en la dirección de Internet proporcionada por el paciente (ver **302** de la figura 3). El portal web **102** con el que el paciente está asociado puede tener la forma de una aplicación de navegador basada en la web o una aplicación descargada de la red **104.** En una realización preferida, esta dirección del portal web puede imprimirse en una tarjeta monedero llevada por el paciente. En realizaciones preferidas adicionales, la información del portal web puede proporcionarse en una tarjeta de banda magnética, un código de barras óptico o código óptico 2-D, un dispositivo de memoria USB u otro medio electrónico portátil de este tipo. En una realización preferida, el acceso al EMR se proporcionará utilizando el portal web **102** como un servidor proxy. Debido a que el Proveedor puede no ser conocido (es decir, ni autentificado ni autorizado) para el EMR, el inicio de sesión de EMR puede estar utilizando credenciales de usuario específicas para el EMR preestablecido para su uso por el portal **102.** Por lo tanto, el acceso puede estar restringido a aquellas funciones del EMR permitidas por el EMR. Por ejemplo, el EMR puede definir el acceso usando este método para que sea 'de solo lectura'.

Una vez iniciada la sesión, el proveedor remoto proporcionará información al portal web que identificará dicho proveedor (véase **303** en la figura 3). Ya sea combinada con esta etapa o como etapa posterior, el proveedor remoto también puede proporcionar información específica del paciente (por ejemplo, identificación del paciente y contraseña/frase de contraseña del paciente). Como se muestra en la figura 3, **303** requiere que el proveedor proporcione información de identificación. Esto se muestra con más detalle en la figura 4. La primera pantalla **400** presentada al proveedor A le permitirá seleccionar el país de registro **401** como se muestra en la figura 4. Como se puede ver en la figura 4, puede haber varias opciones disponibles para que el proveedor de atención médica pueda

seleccionar e identificar la información de identificación relevante del proveedor A. Una vez que se ha seleccionado la información apropiada, el proveedor A se dirigirá a la siguiente pantalla de entrada **500** (véase la figura 5) en la que se debe proporcionar información adicional antes de que el proveedor A pueda continuar. Una vez que se proporciona la información, el portal ubicará al proveedor dentro de un registro maestro de proveedores (MPR) (ver **107** en la figura 1) e intentar localizar los detalles de proveedor aplicables (ver **304** en la figura 3). Como se muestra en la figura 5, se puede requerir que el proveedor A proporcione uno o más de los siguientes en **303:** (a) identificador del proveedor **501;** (b) nombre del proveedor **502;** (c) dirección de ubicación de práctica comercial **503.** Después de la entrada de cualquier información aplicable del proveedor de atención médica por parte del proveedor u otros (por ejemplo, número identificador del proveedor A), el portal web **102** puede acceder al MPR **107** e intentar localizar detalles adicionales del proveedor, incluida la dirección de Práctica Comercial. El REMRAS puede usar la información ingresada por el Proveedor A para mostrar los datos demográficos del proveedor (por ejemplo, información relacionada o específica de ese proveedor) utilizando el MPR, como, por ejemplo, el Registro del Identificador Nacional de Proveedor (NPI) de Estados Unidos. Como otro ejemplo, en Canadá, el Colegio provincial de médicos y cirujanos proporciona un registro provincial. Una búsqueda bajo un número del CPSO (Colegio de Médicos y Cirujanos de Ontario) como en la figura 5 **501** es una realización preferida. En una realización más preferida, el Registro NPI permite a los usuarios de la presente invención, que incluyen tanto individuos como sistemas informáticos, buscar información de un proveedor de atención médica, tal como información de NPPES. Por ejemplo, los usuarios pueden buscar un proveedor por NPI o Nombre Empresarial Legal. Algunos proveedores de servicios de salud proporcionan sus SSN, ITIN del IRS o EIN en secciones de la aplicación de NPI que contienen información que se requiere divulgar según la legislación aplicable. Por ejemplo, los Proveedores que son personas pueden haber informado sobre SSN o ITIN del IRS en campos que se pueden divulgar según la FOIA (como en los campos "Identificadores de otros proveedores" o "Número de licencia"). Una persona incorporada, al solicitar una NPI para la corporación, puede haber informado su SSN como el EIN de la corporación.

El MPR proporcionó campos (incluyendo, pero no limitado a, 'Nombre', 'Identificación del proveedor', 'Dirección de Localización de Práctica Empresarial'), así como el 'país' como se identifica por el Proveedor A y 'departamento' como se introdujo por el Proveedor A que pueden ser capturados por el sistema de la presente invención y pueden almacenarse en una memoria de corto o largo plazo. Una vez que se ha encontrado la información aplicable en el MPR, los detalles del proveedor A se pueden mostrar en la pantalla y se le puede pedir al proveedor que confirme que son correctos. Si la información aplicable no se ha encontrado en el MPR (**503** de la figura 5), el proveedor puede ingresar estos campos manualmente (**305** de la figura 3). Una vez que la información aplicable ha sido encontrada en el MPR o ingresada manualmente y se identifica como correcta, se puede identificar o ingresar el propósito de uso (ver **505**) junto con el departamento **504** del proveedor**.** El proveedor A puede tener que afirmar explícitamente el propósito de uso para el cual se requiere el acceso, tal como, por ejemplo, "Tratamiento de emergencia" y para este fin, se puede presentar un campo de entrada de datos al proveedor A. Una vez que se proporciona la información, el trabajador de salud puede hacer clic en "Siguiente" como se muestra en la figura 5 para pasar a la siguiente pantalla.

Será obvio que el mismo enfoque puede utilizarse para fines de uso que no sea el tratamiento de emergencia, tales como la consulta con proveedores adicionales, entre otros. Un ejemplo puede ser un administrador de EMR que proporciona la identificación del paciente del EMR y una frase de contraseña al consultor como información ingresada por el proveedor. Del mismo modo, el propio paciente puede usar el servicio para acceder a su PHI.

Una vez que la información del proveedor se ha introducido o recuperado, según el caso, el usuario remoto identificado puede entonces ser autentificado y autorizado. Esto comprende al menos dos etapas. El portal web **102** puede solicitar que el usuario remoto proporcione uno o más datos específicos del paciente, tales como, pero sin limitación, una identificación del paciente, una contraseña u otros datos de identificación (**306** de la figura 3). La solicitud de los datos específicos del paciente permite que el usuario remoto sea autentificado y autorizado. Si el usuario remoto tiene tanto la ID del paciente como la frase de contraseña, por ejemplo, el usuario remoto puede ingresar la frase de contraseña en el portal web, en cuyo momento se puede validar la contraseña y se puede determinar si el usuario remoto puede ser autorizado (ver **307** de la figura 3). Como resultado de esta autorización, (a) una respuesta 'Permitir' para permitir el acceso a la PHI del paciente o (b) una respuesta 'Denegar' para indicar que los parámetros de información presentados no son suficientes para permitir al usuario remoto (por ejemplo, proveedor remoto) acceder a la PHI del paciente. Si la frase de contraseña es correcta, se puede requerir que el usuario remoto ingrese el propósito de uso/razón para el acceso (vea **310** de la figura 3). En esta realización, el sistema confirma (ver **311** y **312** de la figura 3) que el paciente ha creado una política de consentimiento (como se indica en este documento). Si existe tal política de consentimiento, entonces el portal web 102 accede al EMR estableciendo una conexión proxy con el EMR (véanse **313** y **314** de la figura 3). En este punto, el usuario remoto tendrá acceso al EMR. Al recibir la respuesta 'Permitir' desde el CVS, el REMRAS enviará un proxy de la interfaz del proveedor al servicio EHR/EMR, donde el Proveedor iniciará sesión utilizando las credenciales del REMRAS. Esto le permite al proveedor autorizado/autentificado ver la PHI del paciente en la medida predeterminada por el EHR/EMR.

En una realización preferida, se entenderá por una persona experta en la técnica relevante que el usuario remoto puede ser el paciente, un proveedor de cuidados médicos, un administrador o cualquier otra persona autentificada y autorizada por el propietario de la PHI contenida en el EMR. Al tener la información específica del paciente (por ejemplo, la identificación del paciente y la frase de contraseña), el usuario remoto ha sido autentificado y autorizado.

En otra realización de la presente invención, el usuario remoto puede no tener toda la información necesaria requerida para ser a la vez autentificado y autorizado. Si el usuario remoto cree que debe tener acceso a la información del paciente, como puede ocurrir cuando el paciente no puede proporcionar una contraseña/frase de contraseña o proporcionar la contraseña/frase de contraseña correcta, entonces el REMRAS puede invocar una realización adicional para autentificar la identidad del proveedor en los casos en que dicha autentificación esté disponible. Tal proveedor de servicio de autentificación puede ser suministrada por una tercera parte mediante mensajería a través de Internet (por ejemplo, Equifax/Anakam, Auththentify o Resilient Networks, etc.). En tales casos, pueden requerirse etapas de autentificación y autorización por separado. En esta realización, el usuario remoto (por ejemplo, el proveedor A) solo puede tener la ID del paciente, que luego se ingresa en el portal web **102** y se valida como correcta (ver **308** de la figura 3). Si la ID del paciente es correcta, el usuario remoto debe estar autentificado (por ejemplo, identificado como el usuario remoto proporcionado en **304**). Durante esta etapa de autentificación **309,** se solicitará información adicional específica del usuario remoto que requerirá que el usuario remoto confirme que es la persona identificada en **304/305.** Si esta etapa de autentificación falla (por ejemplo, el usuario remoto no puede proporcionar la información solicitada y/o requerida), entonces se deniega la autorización y no se concede acceso remoto al EMR correspondiente al usuario remoto. Si esta etapa de autentificación tiene éxito (por ejemplo, el usuario remoto puede proporcionar la información solicitada y/o requerida), entonces se confirma la autorización y el portal web pasa a **310** del proceso visto en la figura 3. La comprobación de CVS confirma que (a) existe una política de consentimiento; y (2) que el acceso del usuario remoto al EMR se realiza en circunstancias que están permitidas de acuerdo con las directivas/política de gestión de consentimiento rellenado previamente de los pacientes de acuerdo con las reglas posteriores adjudicadas en el CVS.

La gestión de consentimiento/validación es un proceso que incluye: (1) permitir a los pacientes establecer preferencias/políticas de privacidad para dirigir quién tendrá acceso a su PHI electrónica, con qué propósito y bajo qué circunstancias; y (2) apoyar la creación dinámica, la gestión y la posterior aplicación de las políticas de privacidad del consumidor/paciente a través de mecanismos de control de acceso. La validación del consentimiento se produce luego de que se hayan creado y almacenado las políticas de consentimiento y privacidad como reglas de validación/adjudicación de consentimiento. Esto puede proporcionarse dentro del portal web (por ejemplo, como un componente del software) o dentro de un sistema externo como un servicio. Se accede al CVS utilizando un protocolo de Internet seguro para la determinación final si se permite el acceso a la PHI del paciente. En una realización preferida, se puede usar el protocolo OASIS XACML, pero se debe entender que también se pueden emplear otros protocolos de solicitud de acceso. En una realización, una realización de la presente invención también puede requerir la selección o inserción de un propósito de uso de la PHI como un atributo de CVS requerido para la validación. En todos los casos, se presentará al proveedor una pantalla de acceso **700** (véase la figura 7) para verificar la identidad del paciente e insertar el motivo de acceso como la etapa final requerida para completar la validación de CVS. Una vez que se cumplen todos los requisitos para la validación de CVS, se conecta al EMR a través de un servidor proxy, preferiblemente a través del portal web **102.** La aceptación de acceso puede hacer que se envíe un mensaje de alerta a la dirección del Oficial de Privacidad designado para el EMR. También puede hacer que se envíe un mensaje de alerta a la dirección de notificación previamente proporcionada por el paciente. Dichos mensajes pueden tener la forma de uno o más de un correo electrónico, mensaje de texto, mensaje de voz, notificación telefónica u otra forma.

La falta de requisitos armonizados a través de varias jurisdicciones no permite un modelo de consentimiento detallado uniforme. Sin embargo, al usar el servicio de gestión de consentimiento dirigido por el paciente, es posible desarrollar un conjunto de reglas para tratar el consentimiento, divulgación de información protegida, auditoría y otros principios del código de privacidad. El consentimiento se aplicará al propósito establecido para la divulgación de información personal y puede aplicarse tan estrecha o tan ampliamente como lo permitan las políticas de consentimiento dirigidas por el paciente. Después de proporcionar la información del proveedor A en **503,** la siguiente etapa puede ser que el Proveedor A ingrese los parámetros deseados, tal como la ID del paciente del sistema EMR y la contraseña, frase de contraseña o clave del paciente. El ID del paciente **601** y la frase de contraseña **602** se solicitarán en la pantalla **600** (véase la figura 6). El Proveedor A puede obtener estos dos directamente del paciente. El paciente puede, por ejemplo, llevar una tarjeta de billetera para proporcionar la URL del REMRAS y la identificación del paciente en el EMR para este fin. La contraseña o frase de contraseña puede provenir de la memoria del paciente o de un tercero. En una realización preferida, puede haber más credenciales del paciente requeridas, tales como la respuesta a una pregunta, o algún otro método de autorización bien conocido usando un secreto conocido solo por el paciente. Si el paciente desea una mayor confidencialidad, el paciente puede ingresar la contraseña o frase de contraseña directamente en el ordenador del Proveedor A sin necesidad de divulgarla al Proveedor A. El ID del paciente en el EMR y la contraseña/frase de contraseña pueden validarse antes de continuar. Esta validación en sí misma no constituye un signo de EMR en operación. La validación de CVS es un requisito adicional antes de iniciar la sesión para ver la PHI del paciente.

Tras la entrada del parámetro o parámetros, el REMRAS autorizará el acceso a la PHI del paciente por parte del proveedor mediante la consulta del servicio de validación de consentimiento (CVS) que puede ser a través de Internet de una manera que es bien conocida (véase **104** de la figura 1). Como parte de una validación de CVS, puede aparecer una pantalla de acceso en la que el Proveedor A debe proporcionar detalles adicionales sobre la razón para tener acceso a la PHI (ver **700** en la figura 7). La información proporcionada por el Proveedor A se usará para crear una pista de auditoría del acceso y se puede usar como atributos para la validación de CVS. En una

realización preferida, también puede hacer que un mensaje, tal como un correo electrónico o mensaje de texto, sea enviado a una persona designada (por ejemplo, un oficial de privacidad) para alertar a uno o más del acceso a la PHI. En una realización preferida adicional, también puede provocar que un mensaje, tal como un mensaje de correo electrónico o un mensaje de texto, sea enviado a uno o más destinos proporcionados por dicho paciente para alertar al paciente sobre acceso de emergencia o de otro tipo a la PHI del paciente.

Aunque aspectos preferidos de la presente invención se han descrito en detalle, diversas modificaciones, alteraciones, y cambios se pueden hacer sin apartarse del alcance de la presente invención como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para permitir que un proveedor no conocido en una red informática tenga acceso a un registro médico electrónico de un paciente almacenado en la red informática, estando el método **caracterizado por**:

(a) el proveedor que solicita acceso al registro clínico electrónico y que proporciona a un proveedor información seleccionada del grupo que consiste en la identificación del proveedor, la ubicación del proveedor, el departamento del proveedor y el propósito del uso, un atributo de CVS seleccionado del grupo que consiste en el nombre del paciente, la identificación del proveedor, la ubicación del proveedor, el departamento del proveedor, el propósito de uso y la razón y una parte de información del paciente seleccionada del grupo que consiste en una identificación del paciente, una contraseña, frase de contraseña y una clave y que proporciona el propósito de uso/razón;

(b) autentificar al proveedor a través de la parte de información del proveedor y dependiente de un servicio de autentificación específico del proveedor;

(c) autentificar al proveedor validando la parte de información del paciente;

(d) confirmar un protocolo de consentimiento específico del paciente basado en:

(i) el atributo de CVS;

(ii) la información del paciente;

(iii) el propósito de uso/razón; y

(e) establecer una conexión para el acceso al registro clínico electrónico para el proveedor dependiendo de una autentificación recibida desde la etapa (c) y una confirmación recibida desde la etapa (d).

2. El método de la reivindicación 1, en el que la identidad del paciente se verifica entre las etapas (b) y (c).

3. El método de la reivindicación 1, en el que el protocolo de consentimiento específico del paciente se basa en una política de consentimiento del paciente.

4. El método de la reivindicación 3, en el que en la etapa (e) el al menos un atributo de CVS y la primera o segunda parte de información del paciente coinciden con la política de consentimiento del paciente.

5. El método de la reivindicación 4, en el que el paciente determina la política de consentimiento del paciente antes de la etapa (a).

6. El método de la reivindicación 5, en el que la política de consentimiento del paciente proporciona las circunstancias bajo las cuales se permite el acceso de un proveedor al registro médico electrónico.

7. El método de la reivindicación 6, en el que el servicio de autentificación del proveedor es una fuente central y autorizada de información del proveedor de servicios de salud.

8. El método de la reivindicación 7, en el que la fuente central y autorizada de información del proveedor de servicios de salud es un registro maestro de proveedores.

9. El método de la reivindicación 8, en el que el registro maestro de proveedores se selecciona del grupo que consiste en el Registro Nacional de Identificadores de Proveedores de Estados Unidos o uno de los Registros de Colegios y Médicos Canadienses.

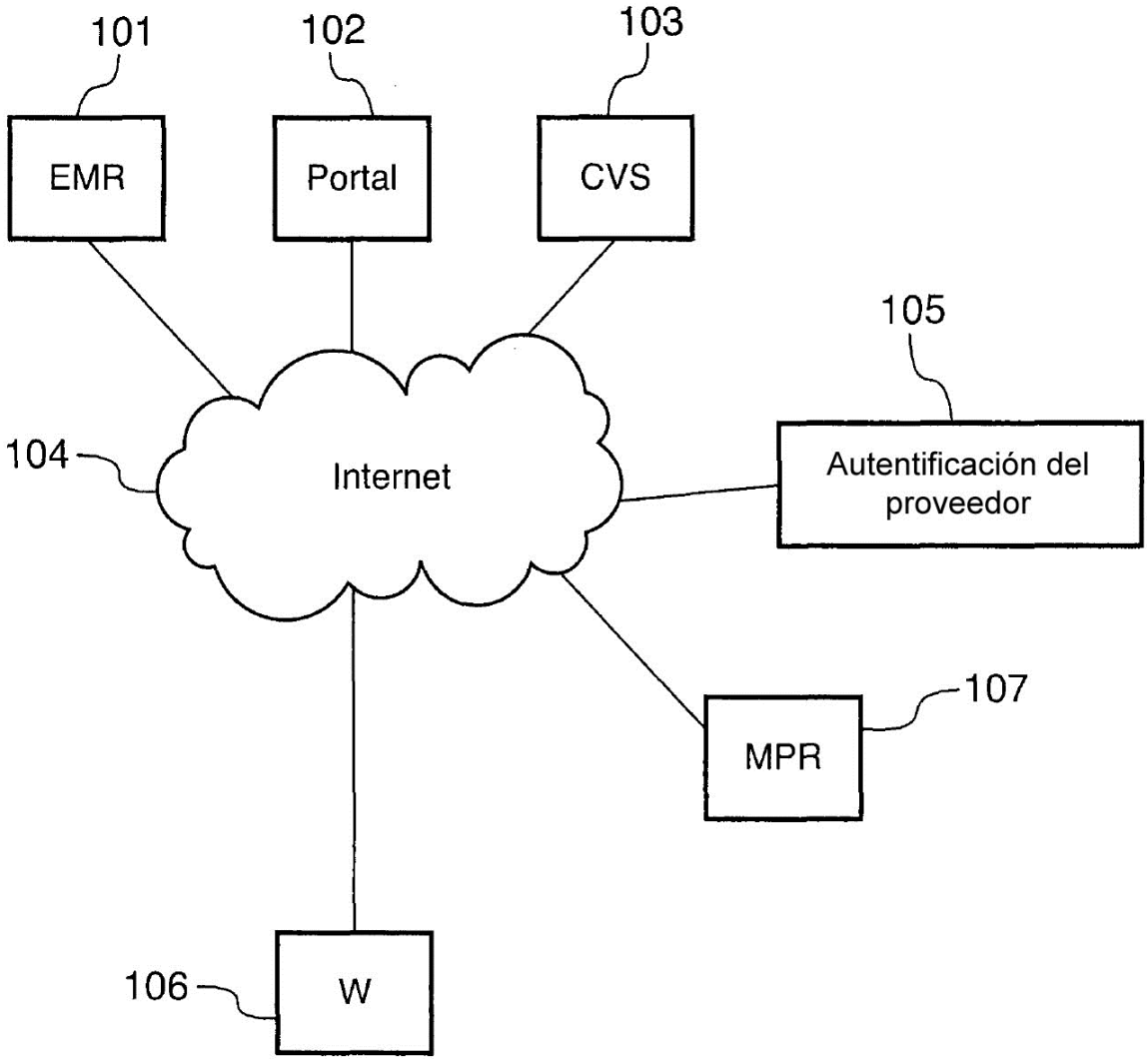
101
102
103
EMR
Portal
CVS
105
104
Internet
Autentificación del proveedor
107
MPR
106
W

FIG.1

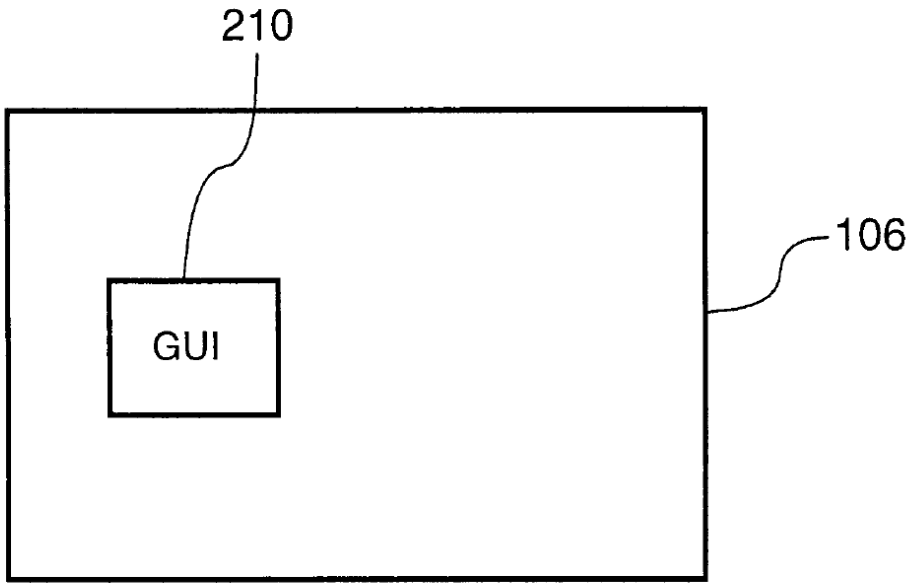

FIG.2

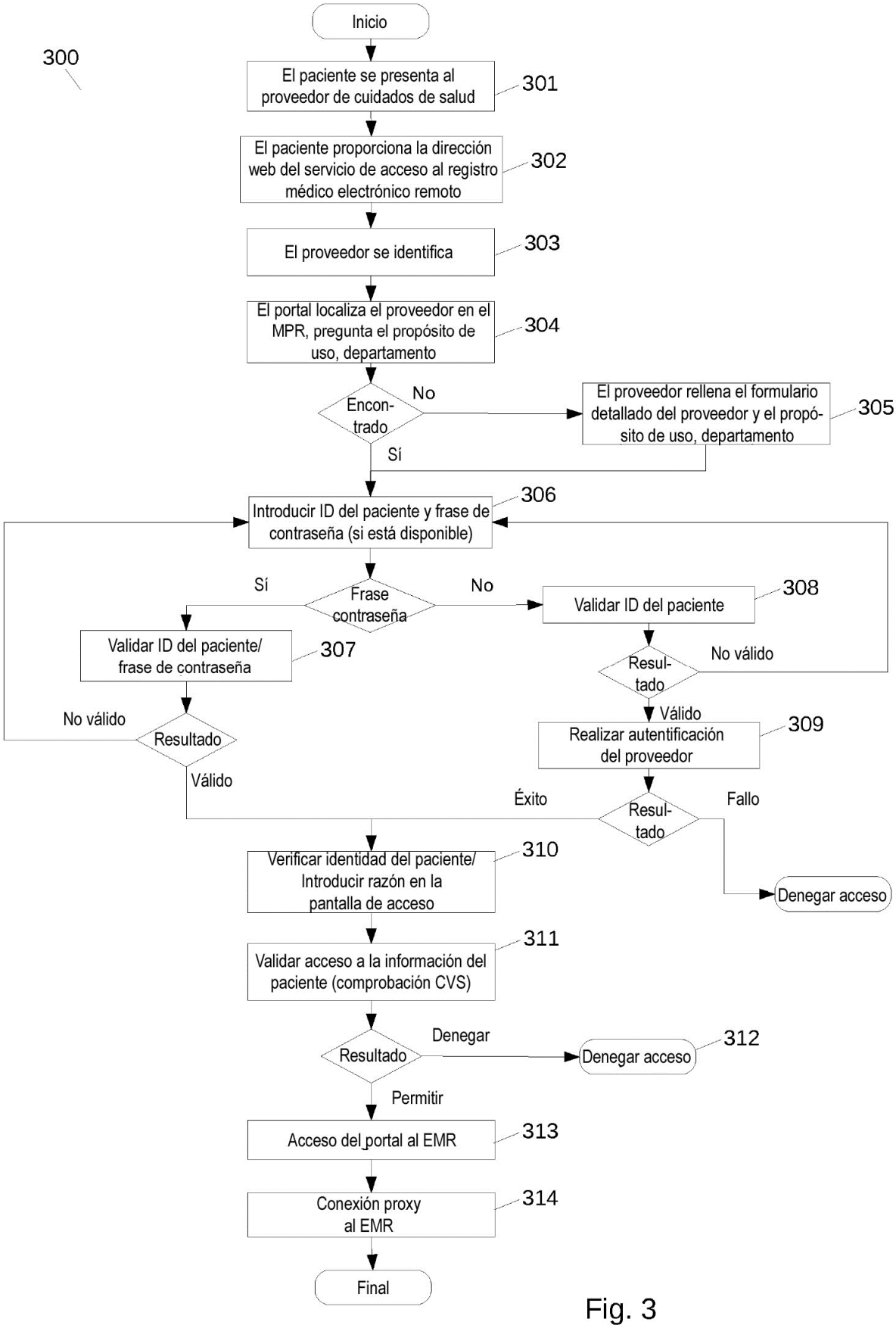
300
Inicio
El paciente se presenta al proveedor de cuidados de salud
301
El paciente proporciona la dirección web del servicio de acceso al registro médico electrónico remoto
302
El proveedor se identifica
303
El portal localiza el proveedor en el MPR, pregunta el propósito de uso, departamento
304
Encon-trado
No
El proveedor rellena el formulario detallado del proveedor y el propósito de uso, departamento
305
Sí
Introducir ID del paciente y frase de contraseña (si está disponible)
306
Sí
Frase contraseña
No
Validar ID del paciente
308
Validar ID del paciente/ frase de contraseña
307
Resul-tado
No válido
Válido
No válido
Resultado
Realizar autentificación del proveedor
309
Válido
Éxito
Resul-tado
Fallo
Verificar identidad del paciente/ Introducir razón en la pantalla de acceso
310
Denegar acceso
Validar acceso a la información del paciente (comprobación CVS)
311
Denegar
Resultado
Denegar acceso
312
Permitir
Acceso del portal al EMR
313
Conexión proxy al EMR
314
Final

Fig. 3

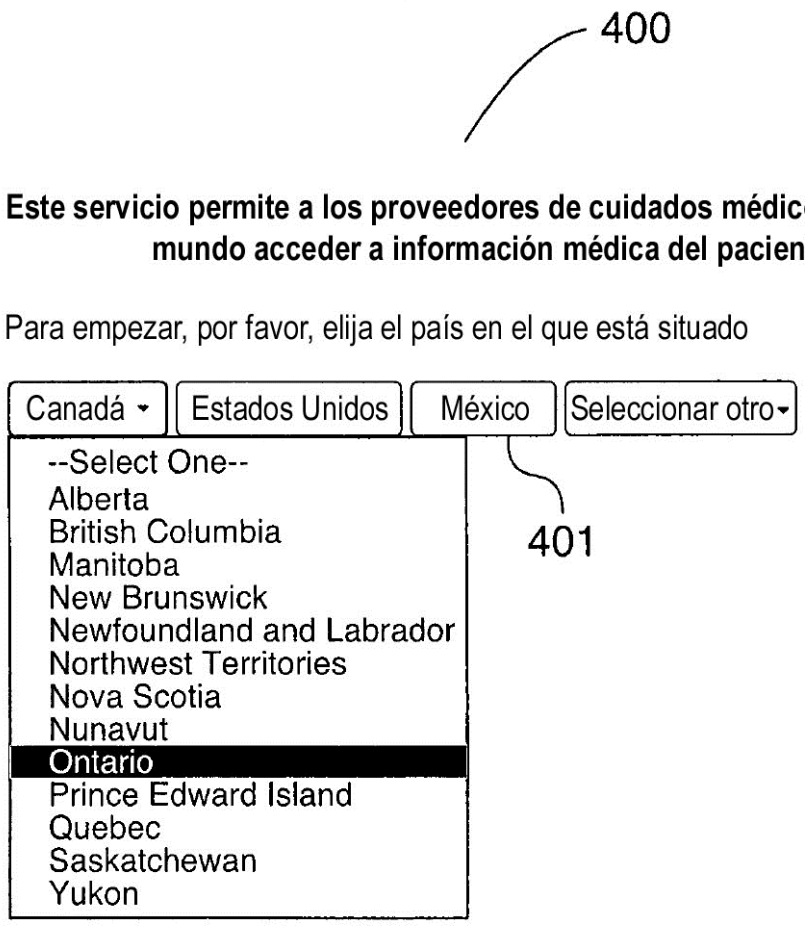
400
Este servicio permite a los proveedores de cuidados médicos en todo el mundo acceder a información médica del paciente
Para empezar, por favor, elija el país en el que está situado
Canadá
Estados Unidos
México
Seleccionar otro
--Select One--
Alberta
British Columbia
Manitoba
New Brunswick
Newfoundland and Labrador
Northwest Territories
Nova Scotia
Nunavut
Ontario
Prince Edward Island
Quebec
Saskatchewan
Yukon
401

FIG.4

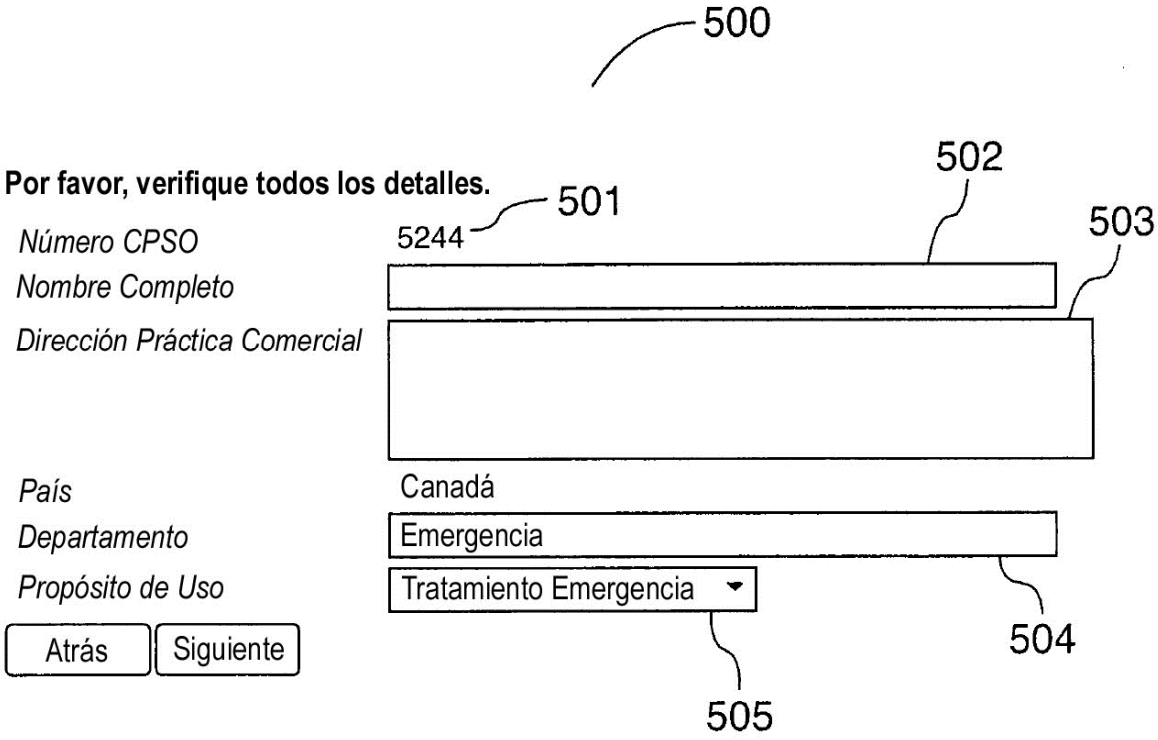
500
Por favor, verifique todos los detalles.
501
502
503
5244
Número CPSO
Nombre Completo
Dirección Práctica Comercial
País
Canadá
Departamento
Emergencia
Propósito de Uso
Tratamiento Emergencia
Atrás
Siguiente
504
505

FIG.5

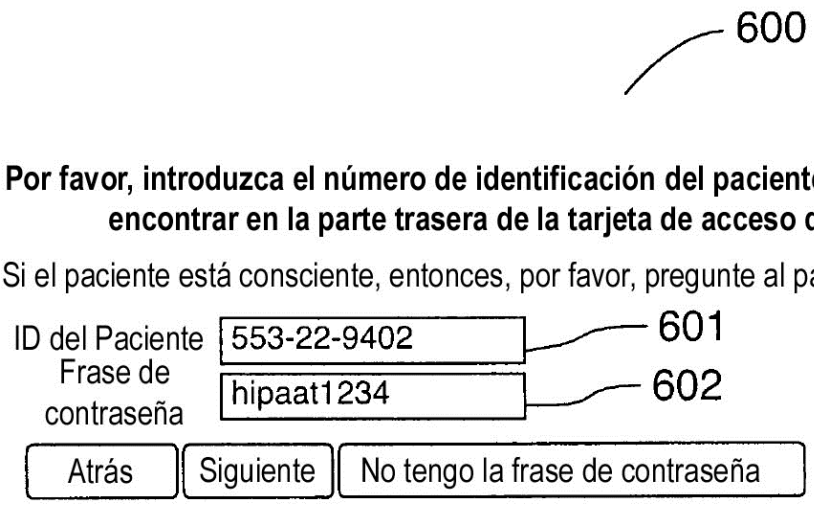
600
Por favor, introduzca el número de identificación del paciente. Esta información se puede encontrar en la parte trasera de la tarjeta de acceso de salud del paciente.
Si el paciente está consciente, entonces, por favor, pregunte al paciente su frase de contraseña.
ID del Paciente
553-22-9402
601
Frase de contraseña
hipaat1234
602
Atrás
Siguiente
No tengo la frase de contraseña

FIG.6

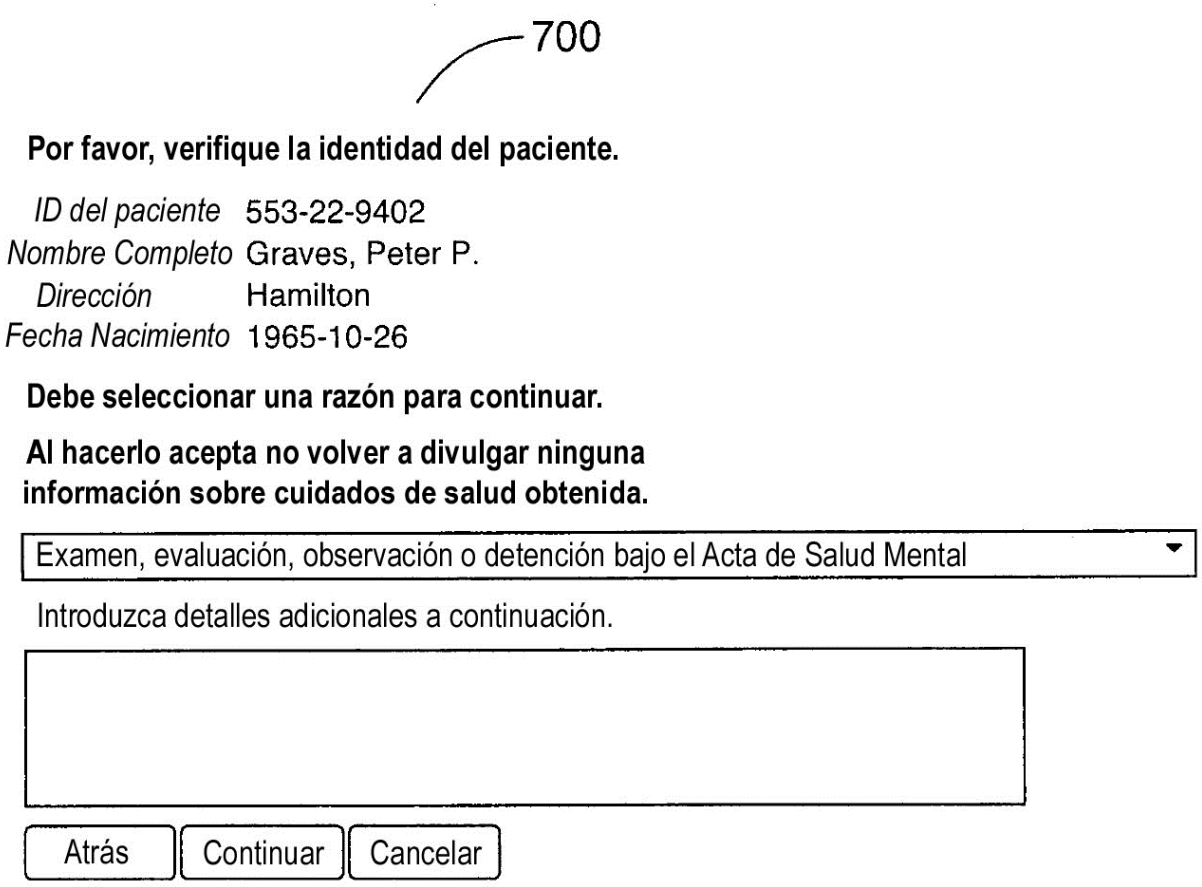
700
Por favor, verifique la identidad del paciente.
ID del paciente 553-22-9402
Nombre Completo Graves, Peter P.
Dirección Hamilton
Fecha Nacimiento 1965-10-26
Debe seleccionar una razón para continuar.
Al hacerlo acepta no volver a divulgar ninguna información sobre cuidados de salud obtenida.
Examen, evaluación, observación o detención bajo el Acta de Salud Mental
Introduzca detalles adicionales a continuación.
Atrás
Continuar
Cancelar

FIG.7