

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 491 491**

21 Número de solicitud: 201330310

51 Int. Cl.:

**G06F 19/00** (2011.01)

**G06Q 50/22** (2012.01)

12

# PATENTE DE INVENCION

B1

22 Fecha de presentación:

**05.03.2013**

43 Fecha de publicación de la solicitud:

**05.09.2014**

Fecha de la concesión:

**09.06.2015**

45 Fecha de publicación de la concesión:

**16.06.2015**

73 Titular/es:

**VODAFONE ESPAÑA, S.A.U. (100.0%)**  
**Avda. de Europa, 1 Parque Empresarial La**  
**Moraleja**  
**28108 Alcobendas (Madrid) ES**

72 Inventor/es:

**ALONSO DÍAZ, Patricia;**  
**ALMODÓVAR HERRÁIZ, Daniel y**  
**ESTEVE ASENSIO, Guillermo**

74 Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

54 Título: **Método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario**

57 Resumen:

Método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario.

La invención propuesta se refiere a un método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario. La invención comprende las etapas de: registrar en un servidor un usuario asociado con un ID y un primer conjunto de metadatos; registrar un dispositivo de monitorización sanitaria asociado con un segundo ID y un segundo conjunto de metadatos; después, enviar a través de un primer canal de comunicación el ID asociado con el usuario y el primer conjunto de metadatos al servidor mediante un dispositivo móvil; tomar una medición del usuario mediante el dispositivo de monitorización sanitaria y enviar a través de un segundo canal de comunicación dicha medición asociada con el segundo ID y el segundo conjunto de metadatos al servidor; comparar los metadatos almacenados en el servidor; y finalmente asociar el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria correspondiente al segundo conjunto de metadatos, basándose la asociación en los resultados de la comparación anterior.

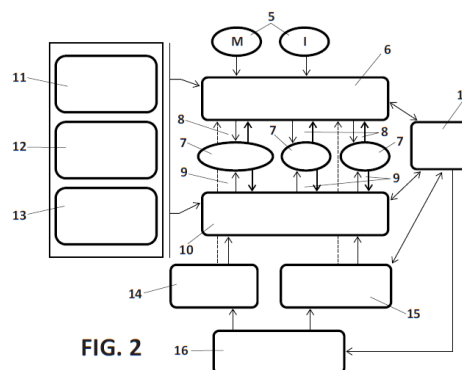


FIG. 2

ES 2 491 491 B1

## DESCRIPCIÓN

Método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario

### **Campo técnico de la invención**

La presente invención tiene aplicación en el campo de la e-Salud y la monitorización de mediciones sanitarias de clientes (pacientes). Más particularmente, la invención se centra en la protección de datos enviados y en garantizar la privacidad del usuario describiendo un método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario.

### **Antecedentes de la invención**

Actualmente, las enfermedades crónicas están aumentando en todo el mundo junto con la necesidad de un control médico de la salud de personas que padecen dichas enfermedades crónicas. El uso de supervisión médica remota ahorra muchos costes.

Existe una amplia variedad de dispositivos sanitarios como medidores de tensión arterial, básculas o glucómetros con capacidad para enviar mediciones de los pacientes de manera remota a los doctores para su supervisión desde hospitales y centros de asistencia o los hogares de los pacientes. Un escenario factible es que se use un único dispositivo sanitario por varios usuarios en un espacio público, tal como una residencia para personas mayores, por tanto es necesario asociar cada medición médica con la persona y es aquí cuando surge el problema acerca del anonimato, y los requisitos específicos de muchos casos.

El estado de la técnica da a conocer algunas invenciones acerca de este tema, por ejemplo el documento US201209676 (A1) "Multiuser health monitoring using biometric identification" (monitorización sanitaria de múltiples usuarios usando identificación biométrica) en el que se presenta una estación central, sistema y método de monitorización sanitaria para monitorizar de manera remota la salud de una persona. Esta patente proporciona un método para emparejar la medición con el identificador de la persona o bien en una estación central local o bien en una remota. Sin embargo, este método puede ser válido cuando los requisitos sobre privacidad y las leyes de protección de datos son poco exigentes, pero es claramente insuficiente para leyes sobre privacidad estrictas, como tienen la mayoría de países europeos en los que los datos médicos se consideran extremadamente sensibles y por tanto requieren métodos específicos de protección.

Las patentes US20120030229A1 y US20110313774A1 describen también un método para asociar medidas con un usuario usando sellos de fecha y hora, pero el principal problema de estas patentes es que una solución basada en sellos de fecha y hora sólo es válida para un reducido grupo de usuarios y no puede garantizarse el anonimato de los usuarios.

Otra solución propuesta en el estado de la técnica es el documento US2009205042A "External user interface based measurement association" (Asociación de medición basada en interfaz de usuario externa), en el que el paciente "se identifica" y hay una etapa de asociar mediciones con ID de pacientes (se usa un "dispositivo remoto" contra un "dispositivo de identificación" que se comunica con un "dispositivo de asociación" que, tras la asociación, transfiere los datos al "servidor de medición", pero todo este proceso implica un único canal de comunicación o, al menos, dos canales estrechamente relacionados, lo que puede poner en riesgo el anonimato. La vinculación usuario-medición se realiza localmente en la "estación de paciente" a pesar del método de sesión descrito. La finalidad de esta solución está lejos de cumplir con las leyes de

protección de datos estrictas sino que parece un método para permitir muchas mediciones de un único usuario útil con fines de una sesión de rehabilitación, como por ejemplo ejercicios de fisioterapia para recuperar un miembro dañado.

5 Por tanto, en el estado de la técnica falta un método para asociar de manera anónima usuarios con las mediciones tomadas por dispositivos de monitorización. Las mediciones y la identificación viajan juntas o están vinculadas de manera evidente en todas las soluciones comentadas anteriormente o incluso se realiza una correspondencia de manera local, lo cual es sumamente inapropiado para garantizar el anonimato del servicio.

10

### **Sumario de la invención**

La presente invención sirve para resolver el problema mencionado anteriormente posibilitando la asociación entre un paciente, que usa un dispositivo móvil, y la medición sanitaria desde un  
15 dispositivo de monitorización que puede usarse por varios usuarios proporcionando anonimato y seguridad. La solución propuesta es que las mediciones y las identificaciones viajen por separado, de manera totalmente descorrelacionada. La asociación tiene lugar únicamente en un servidor que contiene toda la información de los usuarios. Con este fin se presenta un método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario. El  
20 método se caracteriza por que comprende las etapas de:

a) registrar (1) un usuario en un servidor, asignando un primer ID al usuario registrado asociado con un primer conjunto de metadatos;  
b) registrar (2) un dispositivo de monitorización sanitaria en un servidor, asignando un segundo ID al dispositivo de monitorización sanitaria registrado asociado con un segundo conjunto de  
25 metadatos;  
c) enviar (3) a través de un primer canal de comunicación el primer ID y el primer conjunto de metadatos al servidor mediante un dispositivo móvil usado por el usuario;  
d) tomar una medición del usuario mediante el dispositivo de monitorización sanitaria y enviar (4) a través de un segundo canal de comunicación dicha medición asociada con el segundo ID y el  
30 segundo conjunto de metadatos al servidor;  
e) comparar en los metadatos del servidor el primer conjunto de metadatos con todos los conjuntos de metadatos (5) enviados al servidor por dispositivos de monitorización sanitaria registrados en el servidor;  
f) asociar (7) en el servidor el primer ID con las mediciones tomadas mediante el dispositivo de  
35 monitorización sanitaria correspondiente al segundo conjunto de metadatos, basándose la asociación en los resultados de la comparación de la etapa anterior.

La comparación puede afinarse fijando un umbral (14) para los valores de cada uno de los metadatos que van a compararse. Por tanto, pueden obtenerse diferentes series de elementos y  
40 el método se adapta apropiadamente a los diferentes casos.

Los metadatos comparados pueden obtenerse mediante un emparejado directo (6) tanto desde el primer como desde el segundo conjunto de metadatos, aunque adicionalmente, el método también puede comprender reglas de deducción (10) referidas (11, 12, 13) al menos a dos metadatos  
45 específicos.

En una realización de la invención, los metadatos tomados que van a compararse se combinan en grupos de al menos dos elementos. Se asocian condiciones lógicas con dichos elementos basándose en las similitudes.

50

Opcionalmente, la invención puede afinar la comparación aumentando de manera iterativa (9) el número de elementos de metadatos tomados que van a compararse. La asociación que propone

el método puede añadirse finalmente a un archivo histórico asociado con el usuario.

La invención propuesta puede comprender que el dispositivo móvil usado por el usuario y el dispositivo de monitorización sanitaria se comuniquen antes de enviar algo al servidor. El dispositivo móvil, según una realización de la invención es un teléfono móvil y, según una realización particular, la asociación propuesta por la invención se envía al usuario pidiendo su aceptación.

Los metadatos considerados en una realización de la invención se seleccionan de la siguiente lista: hora, fecha, número de serie, frecuencia de uso, luz ambiente, temperatura ambiente, pulsación y movimientos sobre una pantalla, ubicación, datos de redes dentro de alcance o cualquier otro dato recopilado por uno de o tanto el dispositivo de monitorización sanitaria como el dispositivo móvil usado por el usuario. Asimismo, puede incluirse una determinada lógica para comparar metadatos no numéricos.

Un segundo aspecto de la invención se refiere a un sistema para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el sistema caracterizado por que comprende:

- un dispositivo móvil configurado para enviar un primer ID y un primer conjunto de metadatos a un servidor;
- un dispositivo de monitorización sanitaria configurado para tomar una medición del usuario y enviar dicha medición asociada con un segundo ID y un segundo conjunto de metadatos al servidor;
- un servidor configurado para recibir mensajes desde el dispositivo móvil y el dispositivo de monitorización sanitaria, comparar los metadatos incluidos en los mensajes y asociar el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la comparación.

Otro aspecto de la invención se refiere a un servidor para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el servidor caracterizado por recibir mensajes desde un dispositivo móvil y un dispositivo de monitorización sanitaria, comparar los metadatos incluidos en los mensajes y asociar el ID de usuario con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la comparación y una determinada lógica.

Un último aspecto de la invención se refiere a un producto de programa informático que comprende código de programa informático adaptado para realizar el método de la invención cuando dicho código de programa se ejecuta en un ordenador, un procesador de señal digital, una disposición de puertas programables en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

### **Descripción de los dibujos**

Para completar la descripción que está realizándose y con el objetivo de ayudar a entender mejor las características de la invención, según un ejemplo preferido de realización práctica de la misma, acompañando a dicha descripción como parte integrante de la misma, hay un juego de dibujos en los que, a modo de ilustración y de manera no restrictiva, se ha representado lo siguiente:

La figura 1 representa las comunicaciones recibidas por el servidor según una realización de la invención propuesta.

La figura 2 representa el proceso seguido en el servidor para asociar una identificación de usuario con mediciones tomadas por un dispositivo de monitorización sanitaria según una realización de la invención.

**Descripción detallada de la invención**

La invención propuesta posibilita la asociación entre un usuario que usa un dispositivo móvil y una medición sanitaria adquirida mediante dispositivos de monitorización usados por varios usuarios proporcionando anonimato.

Los datos del dispositivo de medición, tal como un dispositivo de medición sanitario, se entregan usando un canal de comunicaciones y los datos para relacionarlos con una persona específica (o paciente) se envían mediante el dispositivo móvil usando un canal diferente. Por tanto, se envían las mediciones y los datos de identificación de manera independiente y totalmente descorrelacionada. Los canales de comunicación usados por el dispositivo móvil pueden variar de una realización a otra. Ejemplos de canales de comunicación usados con este fin son mensajes cortos (SMS), conexiones de datos sobre voz tales como FAX o diferentes protocolos de conexiones sobre datos (correo o STMP, mensajería instantánea o XMPP, petición http, etc.), todos ellos sobre diversas portadoras inalámbricas, tales como WiFi, 3G, LTE, etc. La figura 1 representa claramente este proceso según una realización particular de la invención, en la que tras el registro inicial de los usuarios (1) y dispositivos (2), lo que puede realizarse en cualquier orden, y después de que se les asigne un ID de usuario (21) y un ID de dispositivo (22) respectivamente, ambos elementos empiezan a entregar mensajes al servidor (3), (4). Estos mensajes  $i_i$  (23) y  $m_j$  (24) consisten en varios campos (o vectores) entre los que se incluyen al menos el ID del usuario o el dispositivo respectivamente y algunos elementos de metadatos  $d_i$ ,  $d_j$ . Estos mensajes pertenecen o bien a  $I$  o bien a  $M$ , siendo  $I$  y  $M$  los conjuntos de datos asociados con los usuarios y los dispositivos respectivamente. En el caso del conjunto  $M$ , los vectores  $m_j$  también comprenden las mediciones tomadas.

La figura 2 describe, según una realización particular, el proceso seguido después de que se envíen los mensajes de la figura 1 al servidor. Los conjuntos de datos  $M$  e  $I$  (5) se comparan (6) usando un algoritmo de emparejamiento directo basado en un conjunto de umbrales que definen lo que se considera “muy similar” (14) entre dos metadatos comparables. Los metadatos que van a compararse se definen mediante relaciones lógicas (construidas por ejemplo usando tablas de verdad) entre elementos de los metadatos del mensaje del usuario, denominados  $d_i$  y los metadatos de la medición del dispositivo, denominados  $d_j$  (11) o entre elementos de uno de los conjuntos de datos (12), (13). Esta comparación empieza siendo uno a uno pero evoluciona hasta ser la combinación de muchos a muchos.

Tras esta etapa (6), se generan tres conjuntos (7): un conjunto de pares de mensajes de usuario y mediciones de dispositivo emparejados  $i_i$ ,  $m_j$  y dos conjuntos reducidos de elementos restantes  $M_k'$  e  $I_k'$  por emparejar. Estos tres conjuntos de datos o bien se insertan (8) en el mismo proceso (6) o bien se pasan (9) al proceso complementario de deducción descrito anteriormente (10) que genera un nuevo conjunto  $k$  de tres conjuntos de datos (7). Las iteraciones subsiguientes o bien de un proceso o bien del otro siguen reduciendo el número de elementos en  $M_k'$  e  $I_k'$  al emparejar elementos o marcarlos como errores.

El proceso global se controla mediante un proceso de control (17) que recibe información de los dos procesos mencionados (6) y (10) y de un conjunto de condiciones de detención ajustables (15) para decidir que el estado del proceso (6) o (10) es razonablemente bueno y reglas para marcar elementos como errores o equivocaciones (15). Estas condiciones de parada y reglas pueden ajustarse mediante el proceso de control para definir la siguiente iteración o si habrá otra iteración.

Adicionalmente, los umbrales que definen “muy similar” (14) pueden ajustarse mediante un proceso (16) controlado por el proceso de control (16), afectando al modo en que el proceso (6) y

(10) ejecuta cada iteración.

Los siguientes elementos están incluidos:

- 5 - Un dispositivo móvil (por ejemplo un teléfono móvil) que envía la información del identificador de usuario junto con algunos metadatos. El identificador de usuario (ID) es cualquier dato que conduzca a un usuario previamente registrado en el servicio. Puede ser cualquier cadena de números o de texto, aunque también cualquier patrón biométrico, tal como un patrón de voz, huella dactilar, reconocimiento facial/del iris o similar. Ejemplos de metadatos usados en diferentes realizaciones son ubicación, hora, un identificador de dispositivo (tal como número de serie), tipo y frecuencia de uso del dispositivo y de las aplicaciones en el dispositivo (histórico y actual), luz ambiente, temperatura ambiente, vectores de movimiento y patrones (tal como un signo específico dibujado con el dispositivo móvil), pulsación (sobre la pantalla o botones), imágenes, contactos, datos de redes en uso o dentro de alcance (WiFi, Bluetooth, ID de célula 3G, etc.), pasarelas usadas (conocidas como APN en redes móviles), o cualquier dato recopilado con el dispositivo móvil.
- 10
- 15
- 20 - Un dispositivo de medición, tal como un dispositivo de monitorización sanitaria tal como un medidor de tensión arterial, una báscula, un glucómetro o cualquier otro dispositivo usado para monitorización sanitaria, que toma la medición del usuario. El dispositivo transmite mensajes por cualquiera de los medios mencionados anteriormente como "canales de comunicación". También se considera la posibilidad de conectar dicho dispositivo, según otra realización, al dispositivo móvil del usuario para usar su capacidad y transmitir un mensaje separado y no relacionado. En este último caso, el anonimato es menos estricto que en el procedimiento general descrito debido a que se usa el mismo dispositivo móvil.
- 25
- 30 - Un servidor configurado para recibir las dos informaciones (los datos de identificación del usuario desde el dispositivo móvil y el valor de la medición desde el dispositivo de monitorización sanitaria) y después asociar la identidad del usuario con la medición tomada.
- 35 Según una realización de la presente invención, los usuarios del servicio y los dispositivos asociados con el servicio se registran en un servidor con el fin de usar el método propuesto, de modo que tengan un ID único. Alternativamente, en otra realización de la invención, el ID único se asigna con el primer uso, como un sistema de autoaprovisionamiento.
- 40 Durante el proceso de registro, el usuario asocia su ID de usuario con algunos datos usados como metadatos tal como identificador del ID de dispositivo móvil. Después, durante cada medición, el usuario envía información al servidor para identificarse, por ejemplo dicho ID de dispositivo móvil junto con algunos metadatos de la medición. Aproximadamente al mismo tiempo, el dispositivo de monitorización sanitaria envía al servidor el valor de la medición, algunos metadatos de la medición (como la hora, la ubicación...) y el ID del dispositivo de monitorización sanitaria (por ejemplo la dirección MAC del dispositivo). Después, el servidor reúne esta información y la compara con sus metadatos previamente cargados de cada usuario para asociar el valor del dispositivo de monitorización sanitaria con el ID de usuario correspondiente.
- 45 Los metadatos configurados en el servidor para cada ID de usuario pueden contener adicionalmente los valores históricos de mediciones. Puede usarse una gran serie de metadatos. Como ejemplos de metadatos del dispositivo de medición, puede elegirse cualquiera de la siguiente lista: hora; identificador de dispositivo (tal como número de serie); tipo y frecuencia de uso del dispositivo y de las características en el dispositivo (histórico y actual); luz ambiente (si está disponible); temperatura ambiente (si está disponible); vectores de pulsación y de movimiento y patrones (dependiendo del dispositivo); datos de redes en uso o dentro de alcance (WiFi, Bluetooth, ID de célula 3G, etc.); pasarelas usadas (conocidas como APN en redes móviles) o
- 50

cualquier dato recopilado con el dispositivo; en este último grupo, podría haber cualquier dato proporcionado mediante el dispositivo móvil como la mera proximidad del dispositivo móvil, la ubicación, pulsación (sobre la pantalla o botones); imágenes; contactos; etc. excluyendo el ID de usuario, evidentemente, para garantizar el anonimato.

5

La comparación se realiza en el servidor, que tiene toda la información de todos los usuarios e impide emparejar la información en ningún otro sitio. Escenarios realistas con millones de usuarios demuestran que metadatos basados en la hora sólo son aplicables cuando unos pocos usuarios usan el servicio, en un entorno típico de millones de mensajes concurrentes, la hora tiene poco valor ya que pueden obtenerse miles de mediciones simultáneas con sellos de fecha y hora de relojes no sincronizados que llegan con diferentes tiempos de propagación.

10

Centrándonos en la etapa de comparación, y según esta realización particular, se considera que el conjunto de mediciones  $M$  tiene varios elementos  $m$  igual a largo plazo que el conjunto de elementos de identificación  $i$  del conjunto  $I$ . Normalmente,  $m$  e  $i$  son vectores que contienen varios valores de metadatos además de los valores medidos y la identificación del dispositivo y los usuarios. Se realiza una asociación binaria entre ambos conjuntos minimizando errores. El emparejamiento es iterativo y sobre cada conjunto de metadatos, como el sello de fecha y hora o los valores históricos del usuario usados como ejemplo porque son bastante intuitivos, pero no es secuencial sino inclusivo de modo que tras considerar un metadato, se considera ese mismo y otros. Otros conjuntos de información menos usados son los valores ambientales (redes inalámbricas presentes, presión y temperatura...) medidos en el punto de medición por ambos elementos aproximadamente al mismo tiempo.

15

20

Algunos usuarios son muy predecibles debido a sus metadatos (peso estable/tensión arterial y mediciones regulares desde el mismo sitio a la misma hora) pero algunos de ellos son realmente impredecibles lo que hace la asociación imposible si se aborda individualmente. Sin embargo, aislando dichos usuarios descartando cualquier otra asociación, finalmente se logra un emparejamiento de datos no correlacionados. Según una realización de la invención, dicho emparejamiento no tiene que ser inmediato (en tiempo real) sino que se usan diferentes conjuntos de  $M$  e  $I$  ampliando y contrayendo un intervalo horario y/o área y variando un umbral para cada metadato (por ejemplo, para emparejar todas las mediciones en un determinado intervalo de peso contra todos los ID de usuario usando todos los metadatos disponibles, el umbral para el peso se aumenta cada vez que se ejecuta el método). La comparación de suficientes subconjuntos desequilibrados puede converger para hacer la asociación binaria de los conjuntos equilibrados.

25

30

35

Adicionalmente, los intervalos que van a compararse son mayores o menores (por ejemplo de periodos de tiempo) de modo que los pares no emparejados pueden converger en uno solo considerando un metadato, reduciendo el número de opciones que van a emparejarse considerando otros metadatos hasta alcanzar algún resultado razonable.

40

Algunos otros pares de mensajes son fáciles de emparejar incluso sin conocimiento previo de los hábitos o datos de usuario, como dos mensajes que tienen el mismo conjunto de redes WiFi detectadas entre sus metadatos en un intervalo de tiempo corto. Los metadatos no numéricos requieren una determinada lógica para su comparación. Estos fáciles emparejamientos reducen las opciones para los emparejamientos imposibles y, dados suficientes metadatos e intervalos en cada una, es posible converger en la mayoría de los casos.

45

A continuación se da a conocer un ejemplo específico de implementación:

50 i) El usuario se registra en el servicio para cargar datos desde dispositivos de medición. Esto genera un identificador de usuario (ID de usuario) único para él en el servicio. El servicio proporcionado al usuario consiste en la recepción, almacenamiento y gestión con seguridad de

mediciones relacionadas con él tomadas por cualquiera de los dispositivos que trabajan con el servicio.

ii) Este ID de usuario se usa en dispositivos móviles para indicar al servidor que el usuario ha interactuado con un dispositivo cubierto por el servicio y se han tomado algunas mediciones. El dispositivo móvil es, en este ejemplo, un teléfono inteligente que ejecuta una aplicación en la que el usuario inicia sesión con el ID y tiene un “botón rojo” simplemente para decir “hecho”.

iii) Los dispositivos de medición pueden ser propiedad del usuario o estar disponibles públicamente, por ejemplo una báscula. Este dispositivo está conectado a Internet mediante un medio (por cable o inalámbrico) y tiene capacidad para automatizar el proceso descrito en este ejemplo. Los dispositivos de medición también están registrados en el servicio y también tienen un identificador de dispositivo de medición único; este registro significa que están autorizados a entregar mediciones al servidor.

iv) Una vez realizadas las etapas anteriores, continuando con este ejemplo, el usuario desea pesarse. Por tanto usa una de las básculas registradas en el servicio y se sube a ella. Esto hace que la báscula envíe un mensaje al servidor con la medición y todos los posibles metadatos que rodean la medición.

v) Antes, o después, o mientras está subido a la báscula, el usuario pulsa el “botón rojo” en el teléfono inteligente. Esto hace que el dispositivo envíe un mensaje al servidor con el ID de usuario y todos los posibles metadatos. La lista de metadatos puede ser la misma que la del dispositivo de medición, aunque no necesariamente, ya que el teléfono inteligente y la báscula pueden tener diferentes capacidades para capturar metadatos. Ambos mensajes son totalmente independientes y no están relacionados de modo que con el fin de asociarlos es necesaria una lógica que sólo se ejecuta en el servidor.

vi) Los metadatos, tal como se comentó anteriormente, pueden ser muchas cosas y pueden determinarse mediante varios métodos. Por ejemplo, en cuanto a la ubicación, el teléfono inteligente puede calcularla usando su GPS y la báscula puede tenerla asignada en el servidor. La lista de posibles metadatos ya se ha descrito, aunque algunos de ellos deberían evitarse en uno de los conjuntos de metadatos para garantizar que la correlación entre mensajes (desde el teléfono inteligente y desde la báscula) no pone en riesgo el anonimato de la medición.

vii) En el servidor, hay dos conjuntos de mensajes, un conjunto  $M$  de mediciones procedentes de los dispositivos de medición y otro conjunto  $I$  de identificaciones procedentes de los dispositivos móviles cuando los usuarios pulsaron el botón rojo. El anonimato viene dado no sólo por la entrega no relacionada sino también por el gran número de elementos en ambos conjuntos.

viii) El algoritmo en el servidor compara y empareja tantos pares como sea posible minimizando errores.

Sólo un servidor con todos los mensajes de ambos conjuntos  $M$  e  $I$  puede ejecutar el siguiente proceso con la misma tasa de éxito, de modo que el nivel de protección es realmente alto. Diferentes estrategias proporcionan diferentes tasas de éxito y su combinación conduce a la solución óptima. Las estrategias incluidas son:

- A) Aislar elementos de cada conjunto, de modo que deben emparejarse debido a una correspondencia directa en un metadato específico. Por ejemplo si elementos de cada conjunto muestran la misma lista de redes inalámbricas dentro de alcance con niveles de potencia “muy similares” se emparejan ignorando los sellos de fecha y hora de ambos mensajes.

- B) Emparejar elementos basándose en similitudes en dos o más elementos de los metadatos (por ejemplo la combinación de ubicación y hora). Por motivos de optimización informática, esto se lanza de manera iterativa e incremental.

- C) Usar reglas de deducción derivadas de la lógica, relacionando elementos diferentes de los metadatos para comparar elementos. Por ejemplo, si los metadatos de una identificación de usuario proporcionan una determinada temperatura, debe coincidir con un conjunto de ubicaciones de dispositivos de medición conocidos (en interior, por ejemplo) y horas dependiendo de la estación del año.



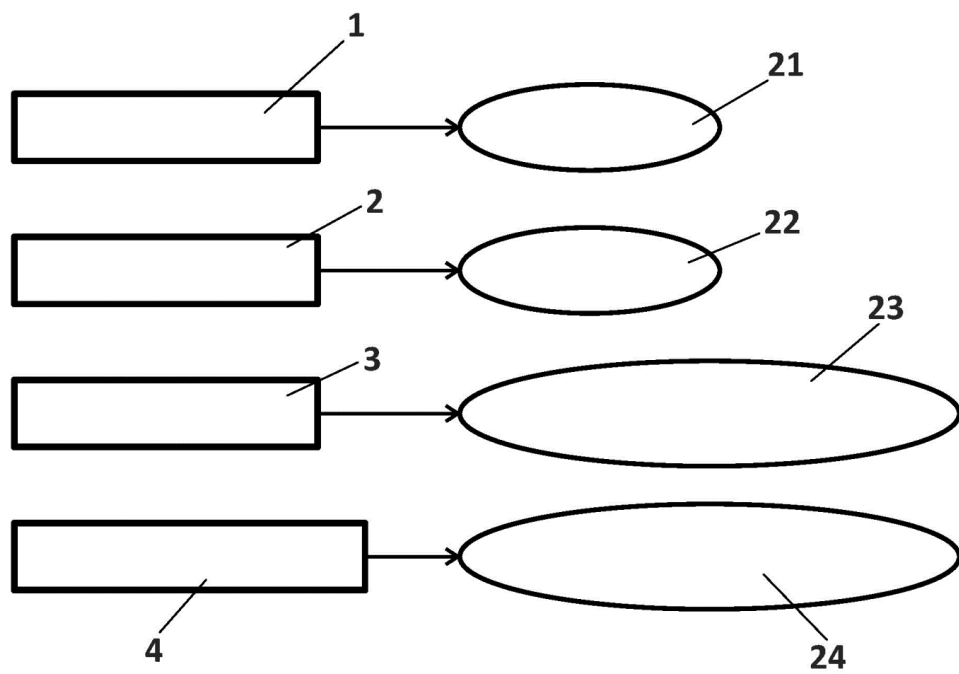
- D) Modificar los intervalos de valores para cada elemento de metadatos aumentando y disminuyendo la definición de valores “muy similares”. Por ejemplo, si hay varios elementos ya emparejados (mediante cualquier estrategia) puede ampliarse el intervalo para incluir simplemente un elemento no emparejado de cada conjunto de modo que puedan emparejarse a pesar de que no hubo una conexión directa entre ellos. Hay algunas reglas lógicas en la definición de intervalo ya que algunos elementos de metadatos no son numéricos, por ejemplo, la lista de redes inalámbricas dentro de alcance requiere una función de ponderación para transformarla en valores comparables por un ordenador. Esto también funciona cuando la adaptación de intervalos de datos da como resultado un elemento de un conjunto contra varios del otro y el servidor lanza entonces un subproceso para elegir el mejor emparejamiento entre ellos. Esto también funciona cuando la definición de “muy similar” se ajusta para dos o más elementos de metadatos al mismo tiempo. De hecho, cuantos más elementos de metadatos estén implicados mejor será la comparación, pero esto debe lanzarse de manera iterativa (aumentado los elementos usados) para optimizar los recursos informáticos.
- E) Marcar emparejamientos imposibles (como opuesto a “muy similar”), de modo que los elementos de ambos conjuntos se reduzcan a un emparejamiento por una correspondencia directa. Esto también puede proporcionar un elemento en un conjunto contra varios en el otro y lanzar un subproceso para hallar el emparejamiento menos malo.
- En una realización de la invención se considera la gestión de mensajes erróneos, lo que afecta al algoritmo para comparar mensajes. Ejemplos de errores son el caso de usuarios que entregan mensajes de “medición tomada” sin tomar realmente ninguna medición y de un dispositivo de medición que toma mediciones de individuos que no están registrados en el servicio. En este caso se define un procedimiento para descartar los mensajes de datos o bien de las mediciones o bien de los usuarios, en el que el usuario debe revisar sus valores históricos más tarde en el servidor mediante un medio telemático tal como una interfaz web por ejemplo, con el fin de aceptar o rechazar dicha medición, o directamente una etapa adicional que consiste en que, una vez que el emparejamiento ha conducido a hacer una asociación usuario-medición, enviar al usuario un mensaje de acuse de recibo desde el servidor pidiendo que se acepte la asociación o corrigiendo la asociación en caso de error. Por ejemplo, el servidor entregará las medidas de valor (por ejemplo el peso) al dispositivo móvil de modo que se visualice y el usuario puede aprobar o rechazar el valor como propio. Otro ejemplo es que el servidor entrega un identificador al dispositivo de medición de modo que el usuario pueda saber si ha sido correctamente identificado y aceptar o rechazar la asociación. Esto aumenta la información recopilada por el servidor y mejora el porcentaje de asociaciones correctas y también, puesto que se proporciona nueva información al sistema, pueden resolverse otras asociaciones erróneas sin la intervención de otros usuarios afectados.
- Otra realización de la invención evita que el dispositivo de medición y/o el dispositivo móvil entreguen su mensaje de manera errónea en caso de que no puedan conseguirse o falten metadatos, como por ejemplo la presencia del otro elemento (ambos elementos difunden su identificador como parte de los metadatos y el otro puede reconocerlo). Aunque esto no significa que la presencia del otro dispositivo deba incluirse en los metadatos.
- El dispositivo de medición puede emplearse por varios usuarios. El dispositivo móvil puede usarse por varios usuarios suponiendo que haya un medio para seleccionar el usuario actual en el mismo, de modo que se seleccione el ID de usuario correcto.
- Por último, la asociación de la identificación de usuario y las mediciones tomadas por los dispositivos de monitorización sanitaria se usa para determinar de manera remota las indicaciones o los tratamientos médicos más apropiados para el usuario. Tal como se ha expuesto, el anonimato es total, de modo que el cliente puede confiar en la privacidad de sus datos y

mediciones sanitarias, que son un tema delicado que no se ha solucionado en el estado de la técnica.

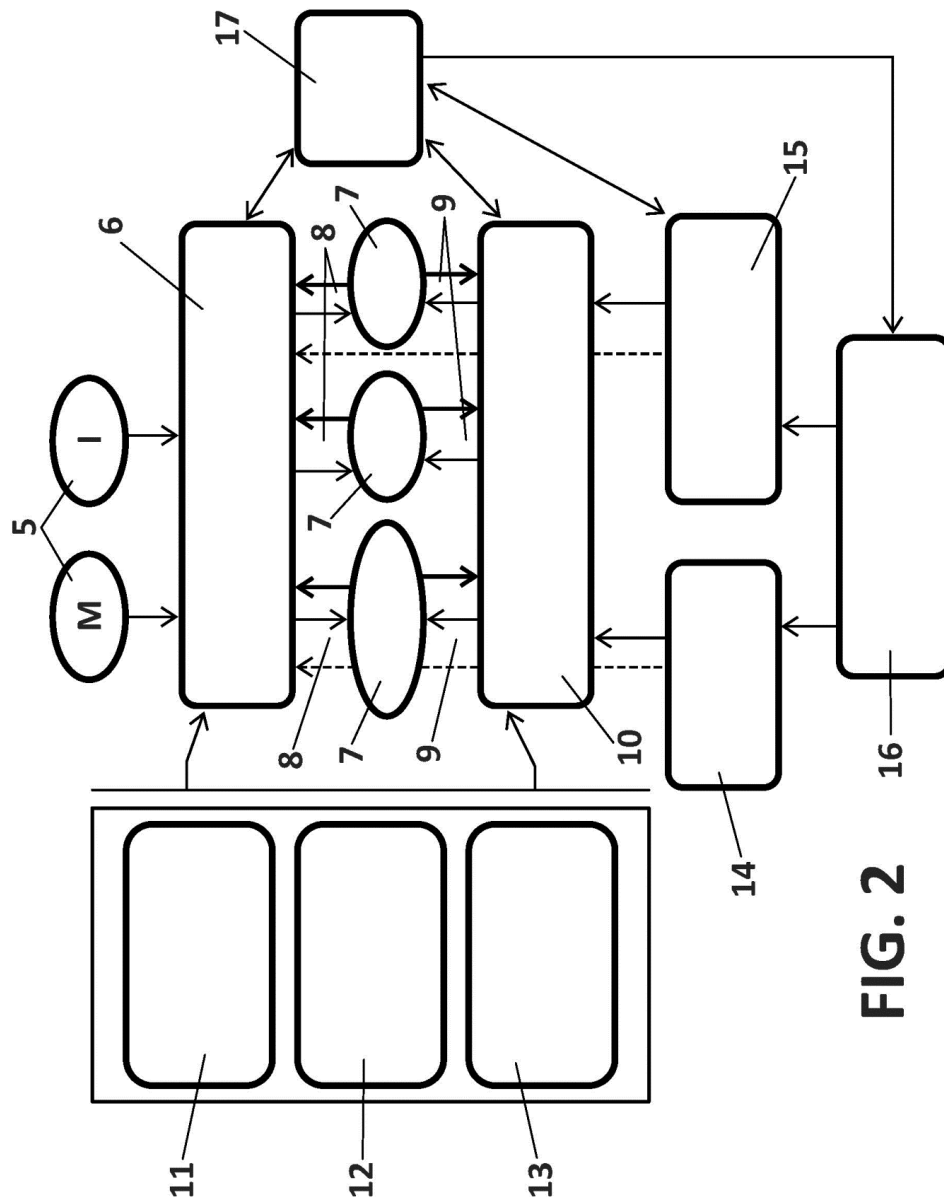
## REIVINDICACIONES

1. Método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el método caracterizado por que comprende las etapas de:  
5 a) registrar (1) un usuario en un servidor, asignando un primer ID al usuario registrado asociado con un primer conjunto de metadatos;  
b) registrar (2) un dispositivo de monitorización sanitaria en un servidor, asignando un segundo ID al dispositivo de monitorización sanitaria registrado asociado con un segundo conjunto de metadatos;  
10 c) enviar (3) a través de un primer canal de comunicación el primer ID y el primer conjunto de metadatos al servidor mediante un dispositivo móvil usado por el usuario;  
d) tomar una medición del usuario mediante el dispositivo de monitorización sanitaria y enviar (4) a través de un segundo canal de comunicación dicha medición asociada con el segundo ID y el segundo conjunto de metadatos al servidor;  
15 e) comparar en los metadatos del servidor el primer conjunto de metadatos con todos los conjuntos de metadatos (5) enviados al servidor por dispositivos de monitorización sanitaria registrados en el servidor;  
f) asociar (7) en el servidor el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria correspondiente al segundo conjunto de metadatos, basándose la  
20 asociación en los resultados de la comparación de la etapa anterior.
2. Método según la reivindicación 1, en el que la comparación de la etapa e) comprende además fijar un umbral (14) para los valores de cada uno de los metadatos que van a compararse.
- 25 3. Método según una cualquiera de las reivindicaciones anteriores, en el que el resultado de la comparación de la etapa e) se refiere a un metadato específico obtenido por un emparejamiento directo (6) tanto del primer como del segundo conjunto de metadatos.
4. Método según una cualquiera de las reivindicaciones anteriores, en el que la etapa de  
30 comparación e) comprende además reglas de deducción (10) referidas (11, 12, 13) al menos a dos metadatos específicos.
5. Método según una cualquiera de las reivindicaciones anteriores, en el que los metadatos tomados para la comparación de la etapa e) se combinan en grupos de al menos dos elementos.
- 35 6. Método según la reivindicación 5, que comprende además afinar la comparación de la etapa e) aumentando de manera iterativa (9) el número de metadatos tomados que van a compararse.
7. Método según una cualquiera de las reivindicaciones anteriores, en el que el dispositivo  
40 móvil usado por el usuario y el dispositivo de monitorización sanitaria difunden un identificador como parte de los metadatos y esperan hasta reconocer el identificador difundido por el otro antes de enviar algo al servidor.
8. Método según una cualquiera de las reivindicaciones anteriores, en el que los metadatos  
45 se seleccionan de la siguiente lista: hora, fecha, número de serie, frecuencia de uso, luz ambiente, temperatura ambiente, pulsación y movimientos sobre una pantalla, ubicación, datos de redes dentro de alcance o cualquier otro dato recopilado tanto por el dispositivo de monitorización sanitaria como por el dispositivo móvil usado por el usuario.
- 50 9. Método según una cualquiera de las reivindicaciones anteriores, en el que el dispositivo móvil usado por el usuario es un dispositivo informático portátil con capacidad de comunicación como un teléfono móvil o una tableta.

10. Método según una cualquiera de las reivindicaciones anteriores, que comprende además la etapa de enviar la asociación de la etapa f) al usuario pidiendo su aceptación.
- 5 11. Método según una cualquiera de las reivindicaciones anteriores, que comprende además añadir las asociaciones de la etapa f) a un archivo histórico asociado con el usuario.
12. Método según una cualquiera de las reivindicaciones anteriores, en el que la etapa e) comprende además una determinada lógica para comparar metadatos no numéricos.
- 10 13. Sistema para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el sistema caracterizado porque comprende:
  - un dispositivo móvil configurado para enviar a través de un primer canal de comunicación un primer ID y un primer conjunto de metadatos a un servidor;
  - 15 - un dispositivo de monitorización sanitaria configurado para tomar una medición del usuario y enviar a través de un segundo canal de comunicación dicha medición asociada con un segundo ID y un segundo conjunto de metadatos al servidor;
  - un servidor configurado para recibir mensajes desde el dispositivo móvil y el dispositivo de monitorización sanitaria, comparar metadatos incluidos en los mensajes y asociar el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la etapa de comparación.
- 20 14. Servidor para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el servidor caracterizado por recibir mensajes desde un dispositivo móvil y un dispositivo de monitorización sanitaria, comparar los metadatos incluidos en los mensajes y asociar el ID de usuario con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la etapa de comparación y una determinada lógica.
- 25 15. Producto de programa informático que comprende código de programa informático adaptado para realizar el método según cualquiera de las reivindicaciones 1-12, cuando dicho código de programa se ejecuta en un ordenador, un procesador de señal digital, una disposición de puertas programables en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.
- 30



**FIG. 1**



**FIG. 2**



- ②① N.º solicitud: 201330310  
②② Fecha de presentación de la solicitud: 05.03.2013  
③② Fecha de prioridad:

## INFORME SOBRE EL ESTADO DE LA TÉCNICA

⑤① Int. Cl.: **G06F19/00** (2011.01)  
**G06Q50/22** (2012.01)

### DOCUMENTOS RELEVANTES

Categoría	⑤⑥ Documentos citados	Reivindicaciones afectadas
X	US 2012030229 A1 (JI LUSHENG et al.) 02.02.2012, párrafos [0023-0066]; figuras 1-3,20.	1-15
X	US 2009205042 A1 (ZHOU BRIAN et al.) 13.08.2009, párrafos [0001-0050]; figuras 2-5.	1-15
A	US 2009144021 A1 (KETSKES ANDRAS) 04.06.2009, párrafos [0002-0023].	1-15
A	WO 03050729 A2 (EURO CELTIQUE SA et al.) 19.06.2003, página 1, línea 5 – página 23, línea 15.	1-15

#### Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

#### El presente informe ha sido realizado

☒ para todas las reivindicaciones

☐ para las reivindicaciones nº:

Fecha de realización del informe  
27.02.2014

Examinador  
A. Casado Fernández

Página  
1/6

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, G06Q

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC



Fecha de Realización de la Opinión Escrita: 27.02.2014

**Declaración****Novedad (Art. 6.1 LP 11/1986)**

Reivindicaciones 1-12, 15

**SI**

Reivindicaciones 13-14

**NO****Actividad inventiva (Art. 8.1 LP11/1986)**

Reivindicaciones

**SI**

Reivindicaciones 1-15

**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

**Base de la Opinión.-**

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

**1. Documentos considerados.-**

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2012030229 A1 (JI LUSHENG et al.)	02.02.2012
D02	US 2009205042 A1 (ZHOU BRIAN et al.)	13.08.2009
D03	US 2009144021 A1 (KETSKE ANDRAS)	04.06.2009
D04	WO 03050729 A2 (EURO CELTIQUE SA et al.)	19.06.2003

**2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración****Reivindicación 1:**

Método para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario ([0023]-[0026]), estando el método caracterizado por que comprende las etapas de:

- a) registrar un usuario en un servidor, asignando un primer ID al usuario registrado asociado con un primer conjunto de metadatos;
- b) registrar un dispositivo de monitorización sanitaria en un servidor, asignando un segundo ID al dispositivo de monitorización sanitaria registrado asociado con un segundo conjunto de metadatos;
- c) enviar a través de un primer canal de comunicación el primer ID y el primer conjunto de metadatos al servidor mediante un dispositivo móvil usado por el usuario ([0025]-[0026]);
- d) tomar una medición del usuario mediante el dispositivo de monitorización sanitaria ([0023]) y enviar (4) a través de un segundo canal de comunicación dicha medición asociada con el segundo ID y el segundo conjunto de metadatos al servidor ([0023]-[0026]);
- e) comparar en los metadatos del servidor el primer conjunto de metadatos con todos los conjuntos de metadatos enviados al servidor por dispositivos de monitorización sanitaria registrados en el servidor ([0031]-[0032]);
- f) asociar en el servidor el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria correspondiente al segundo conjunto de metadatos, basándose la asociación en los resultados de la comparación de la etapa anterior ([0025]-[0026], [0051]).

La diferencia entre D01 y la reivindicación 1 es que en la reivindicación 1 se especifica el registro de un usuario en un servidor, asignando un primer ID al usuario y el registro de un dispositivo de monitorización sanitaria en un servidor, asignando un segundo ID al dispositivo de monitorización sanitaria.

El efecto técnico de esta diferencia es el registro de un usuario y de un dispositivo en el servidor.

El problema técnico es por lo tanto cómo registrar al usuario y al dispositivo.

En D01 se asignan identificadores al dispositivo del usuario y al dispositivo médico, los cuales son enviados al servidor.

El registro de un usuario o de un dispositivo en un servidor es una técnica habitual ampliamente conocida en el estado de la técnica.

Por tanto, se considera que un experto en la materia aplicaría estas etapas sin hacer uso de la actividad inventiva.

Consecuentemente que la reivindicación 1 no implica actividad inventiva (Artículo 8 LP.).

**Reivindicación 2:**

Método según la reivindicación 1, en el que la comparación de la etapa e) comprende además fijar un umbral ([0064]) para los valores de cada uno de los metadatos que van a compararse.

Por tanto, la reivindicación 2 no implica actividad inventiva (Artículo 8 LP.).

**Reivindicación 3:**

Método según una cualquiera de las reivindicaciones anteriores, en el que el resultado de la comparación de la etapa e) se refiere a un metadato específico obtenido por un emparejamiento directo ([0031]-[0032], [0065]-[0066]) tanto del primer como del segundo conjunto de metadatos.

Consecuentemente, la reivindicación 3 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 4:

Método según una cualquiera de las reivindicaciones anteriores, en el que la etapa de comparación e) comprende además reglas de deducción referidas al menos a dos metadatos específicos (figura 20, [0031]-[0032], [0051], [0065]-[0066]).

Consecuentemente, la reivindicación 4 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 5:

Método según una cualquiera de las reivindicaciones anteriores, en el que los metadatos tomados para la comparación de la etapa e) se combinan en grupos de al menos dos elementos ([0031]-[0032], [0065]-[0066]).

Por lo tanto, la reivindicación 5 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 6:

Método según la reivindicación 5, que comprende además afinar la comparación de la etapa e) aumentando de manera iterativa (9) el número de metadatos tomados que van a compararse.

La repetición de un proceso de forma iterativa no se considera que confiera ningún elemento de significación inventiva con respecto al estado de la técnica conocido.

Por consiguiente, la reivindicación 6 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 7:

Método según una cualquiera de las reivindicaciones anteriores, en el que el dispositivo móvil usado por el usuario y el dispositivo de monitorización sanitaria difunden un identificador como parte de los metadatos ([0023]-[0026]) y esperan hasta reconocer el identificador difundido por el otro antes de enviar algo al servidor ([0025]).

Por consiguiente, la reivindicación 7 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 8:

Método según una cualquiera de las reivindicaciones anteriores, en el que los metadatos se seleccionan de la siguiente lista: hora, fecha, número de serie, frecuencia de uso, luz ambiente, temperatura ambiente, pulsación y movimientos sobre una pantalla, ubicación, datos de redes dentro de alcance o cualquier otro dato recopilado tanto por el dispositivo de monitorización sanitaria como por el dispositivo móvil usado por el usuario ([0033]-[0034]).

Por lo tanto, la reivindicación 8 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 9:

Método según una cualquiera de las reivindicaciones anteriores, en el que el dispositivo móvil usado por el usuario es un dispositivo informático portátil con capacidad de comunicación como un teléfono móvil o una tableta ([0026]).

Por consiguiente, la reivindicación 9 no implica actividad inventiva (Artículo 8 LP.).

## Reivindicación 10:

La reivindicación 10 incluye la etapa de enviar la asociación al usuario pidiendo su aceptación.

El intercambio información con el usuario y la aceptación del usuario son operaciones habituales en el tratamiento de información entre un dispositivo móvil y un servidor.

Esta etapa se considera una variante conocida dentro del alcance de la práctica habitual seguida por el experto en la materia.

Por lo tanto la reivindicación 10 carece de actividad inventiva (Artículo 8 LP.).

## Reivindicación 11:

Método según una cualquiera de las reivindicaciones anteriores, que comprende además añadir las asociaciones de la etapa f) a un archivo histórico asociado con el usuario ([0033]).

Por lo tanto la reivindicación 11 carece de actividad inventiva (Artículo 8 LP).

## Reivindicación 12:

Método según una cualquiera de las reivindicaciones anteriores, en el que la etapa e) comprende además una determinada lógica para comparar metadatos no numéricos ([0065]-[0066]).

Por lo tanto la reivindicación 12 carece de actividad inventiva (Artículo 8 LP).

## Reivindicación 13:

Sistema para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el sistema caracterizado porque comprende:

- un dispositivo móvil configurado para enviar a través de un primer canal de comunicación un primer ID y un primer conjunto de metadatos a un servidor ([0026]-[0028]);
- un dispositivo de monitorización sanitaria configurado para tomar una medición del usuario y enviar a través de un segundo canal de comunicación dicha medición asociada con un segundo ID y un segundo conjunto de metadatos al servidor ([0023]-[0026]);
- un servidor configurado para recibir mensajes desde el dispositivo móvil y el dispositivo de monitorización sanitaria, comparar metadatos incluidos en los mensajes y asociar el primer ID con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la etapa de comparación ([0023]-[0032]).

Por lo tanto la reivindicación 13 carece de novedad (Artículo 6 LP).

## Reivindicación 14:

Servidor para asociar de manera anónima mediciones de un dispositivo de monitorización sanitaria con un ID de usuario, estando el servidor caracterizado por recibir mensajes desde un dispositivo móvil y un dispositivo de monitorización sanitaria, comparar los metadatos incluidos en los mensajes y asociar el ID de usuario con las mediciones tomadas mediante el dispositivo de monitorización sanitaria según el resultado de la etapa de comparación y una determinada lógica ([0023]-[0066]; figuras 1-3, 20).

Por lo tanto la reivindicación 14 carece de novedad (Artículo 6 LP).

## Reivindicación 15:

Producto de programa informático que comprende código de programa informático adaptado para realizar el método según cualquiera de las reivindicaciones 1-12, cuando dicho código de programa se ejecuta en un ordenador, un procesador de señal digital, una disposición de puertas programables en campo, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

La reivindicación 15 es una reivindicación tipo declarativa y carece de actividad inventiva en la medida en que la reivindicación 1 no implica actividad inventiva.

Por lo tanto la reivindicación 15 carece de actividad inventiva (Artículo 8 LP).