(12) UK Patent Application (19) GB (11) 2509064 (13) A

(43) Date of A Publication 25.06.2014

(21) Application No: 1222856.5

(22) Date of Filing: 18.12.2012

(71) Applicant(s):
CompleteGP Limited
(Incorporated in Ireland)
Waterloo House, Mallow, Co Cork, Ireland

(72) Inventor(s):
Carl Beame

(74) Agent and/or Address for Service:
PurdyLucey Intellectual Property
Suite 138/139, The Capel Building, Mary's Abbey,
Dublin 7, Ireland

(51) INT CL:
G06F 21/62 (2013.01) ***G06Q 50/24*** (2012.01)

(56) Documents Cited:
GB 2479074 A **JP 2003296453 A**
US 20090055924 A1

(58) Field of Search:
INT CL **G06F, G06Q**
Other: **Online: WPI, EPODOC**

(54) Title of the Invention: **Method and system for distributing health data**
Abstract Title: **Method and system for distributing health data**

(57) A method of distributing health data, a distributed health record system and program implementing same, are disclosed. The invention is concerned with securely accessing patient or health data of an individual when emergency healthcare is required. At least one portable computer–readable medium 20 has a unique identifier 22 and a respective encryption key, and stores encrypted health data of an individual and decryption means. A server 108 connected to a network stores the or each unique identifier and the or each respective encryption key. When the medium is read by a computing device 101 connected to the network for accessing the encrypted health data stored therein, an authorization token is obtained at the server from the decryption means, and the respective encryption key of the medium is obtained from the server with the decryption means based on the authorization token, whereby the encrypted health data can then be decrypted with the respective encryption key received.

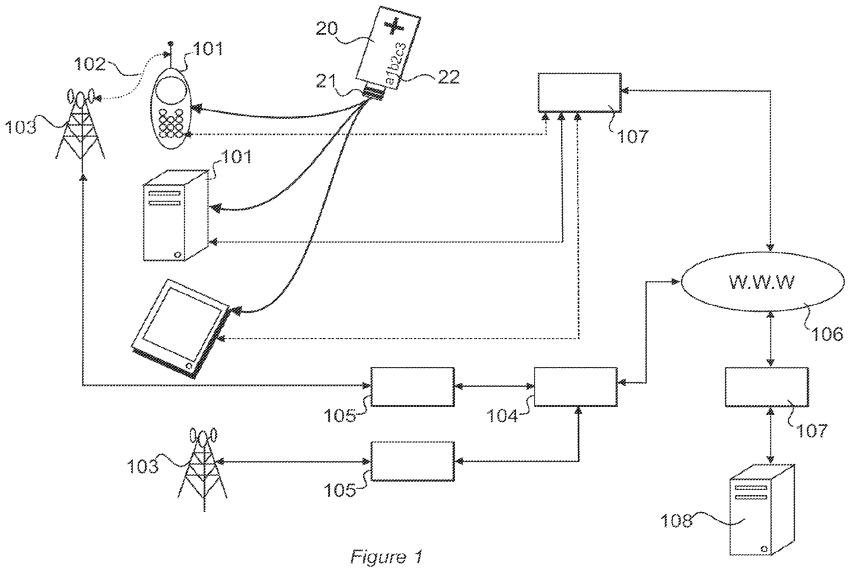

Figure 1

GB 2509064 A

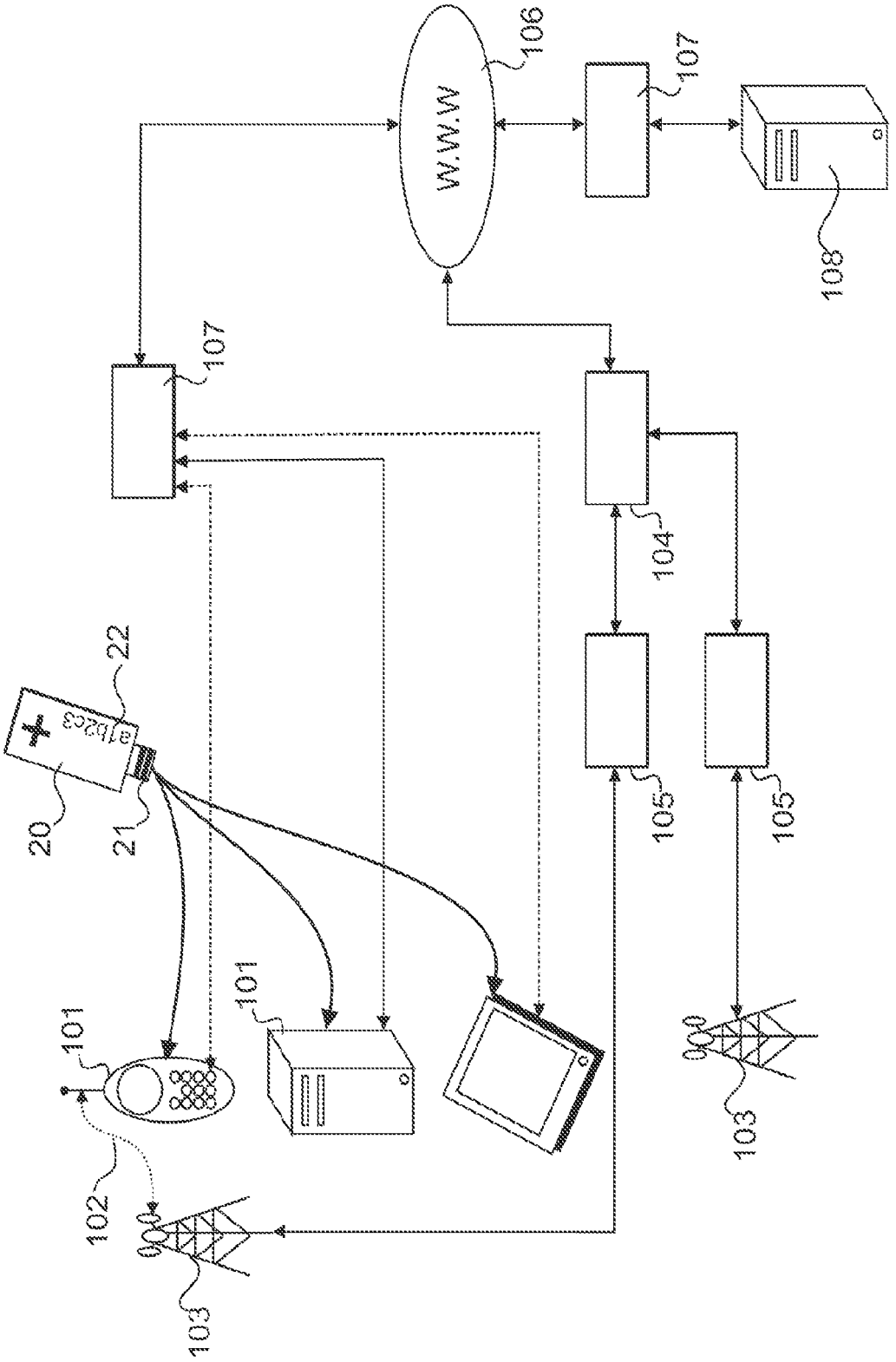

Figure 1

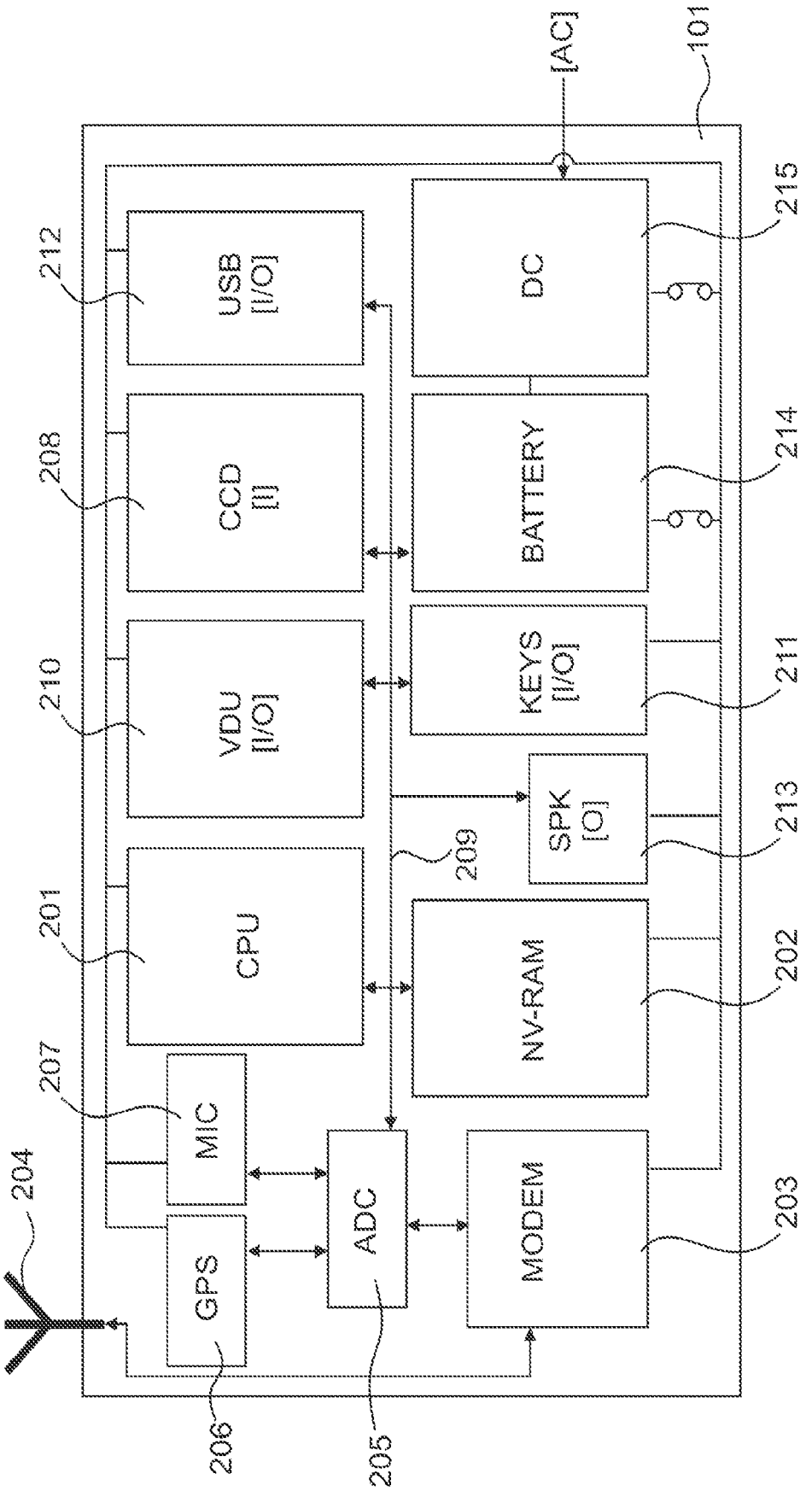
101
[AC]
215
DC
212
USB [I/O]
208
CCD [I]
214
BATTERY
210
VDU [I/O]
211
KEYS [I/O]
213
SPK [O]
209
201
CPU
202
NV-RAM
207
MIC
203
MODEM
204
GPS
ADC
206
205

Figure 2

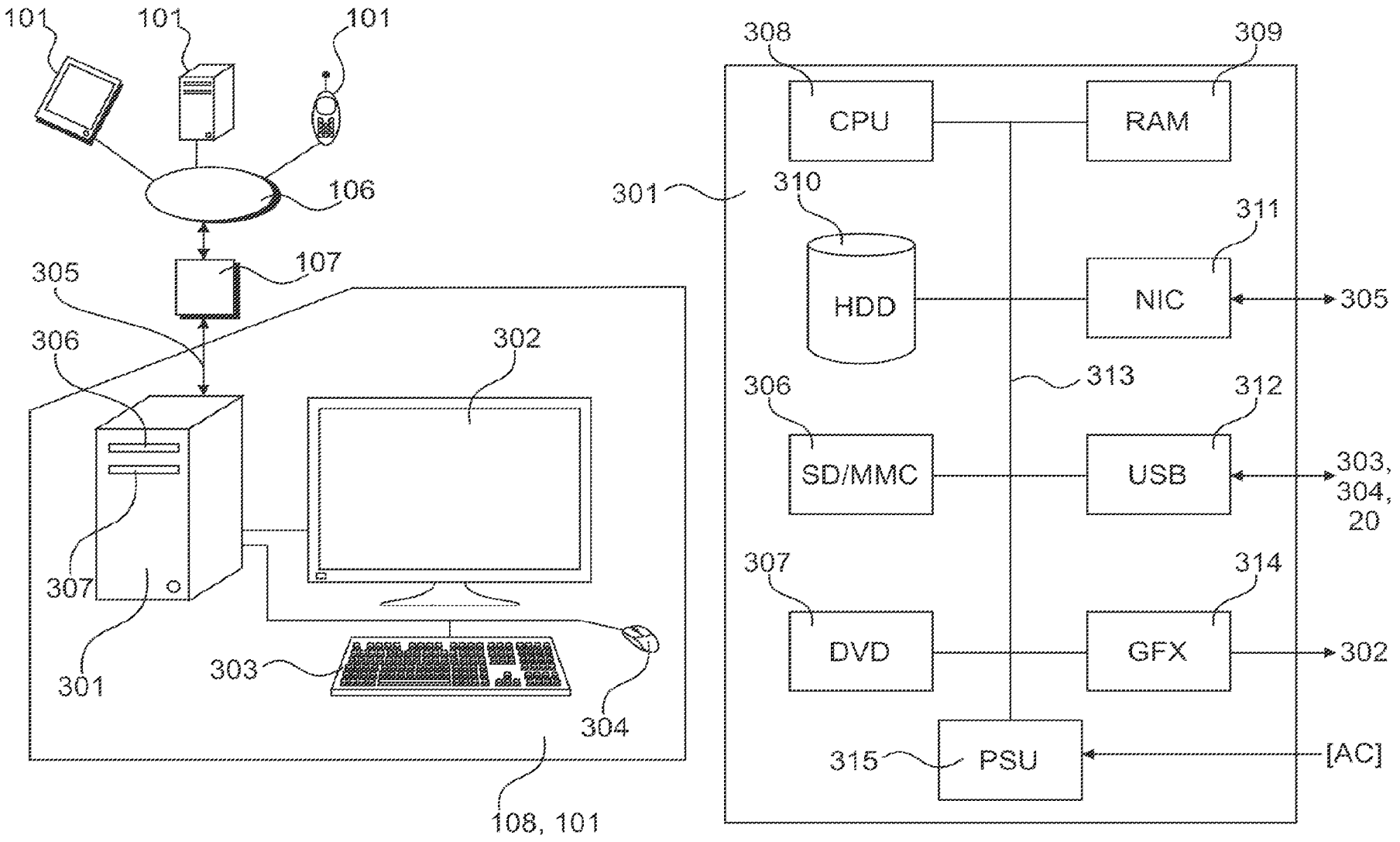
101
101
101
106
107
305
306
302
307
301
303
304
108, 101
308
309
CPU
RAM
301
310
311
HDD
NIC
305
306
313
312
SD/MMC
USB
303,
304,
20
307
314
DVD
GFX
302
315
PSU
[AC]

Figure 3

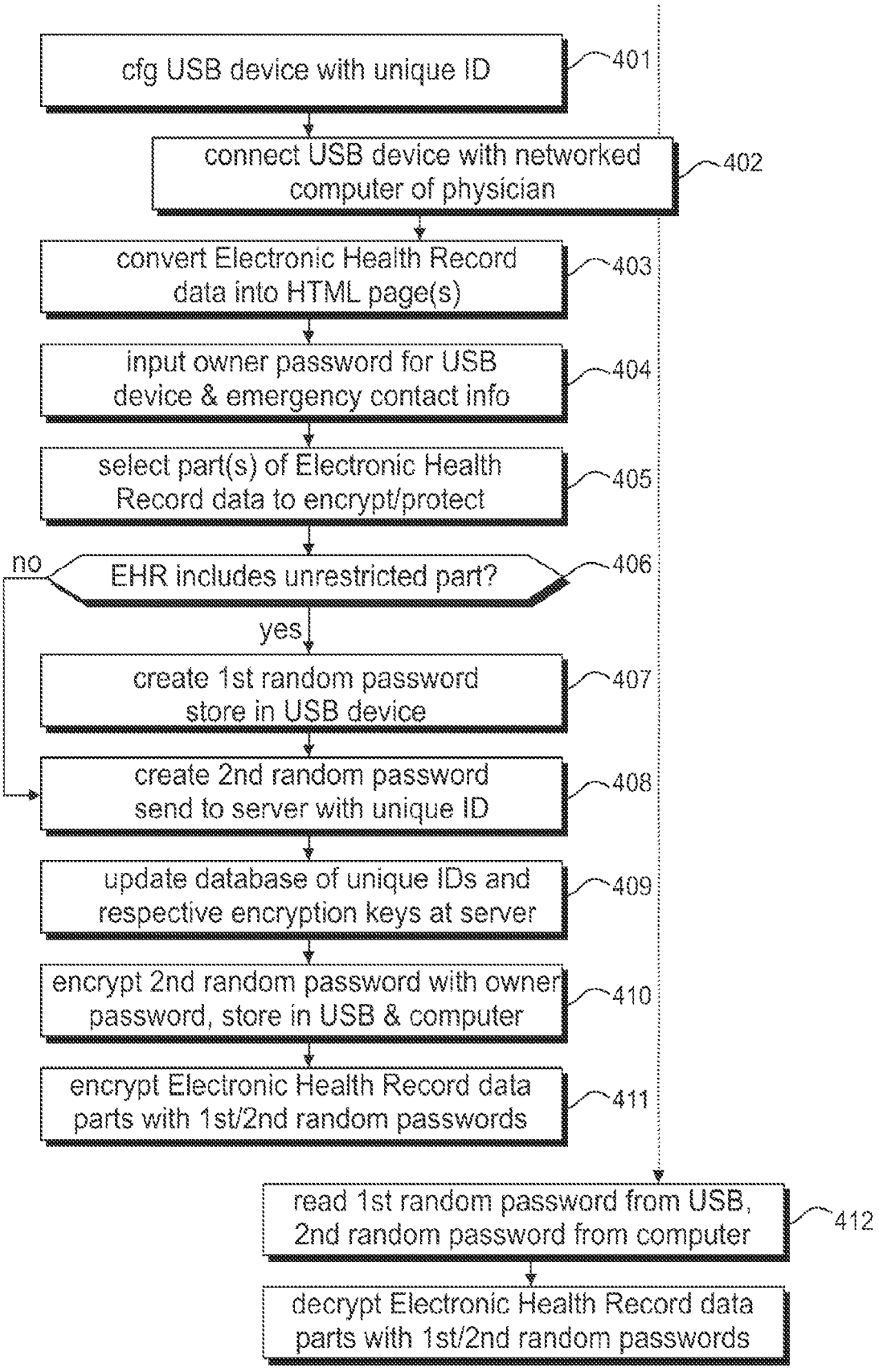
cfg USB device with unique ID
401
connect USB device with networked computer of physician
402
convert Electronic Health Record data into HTML page(s)
403
input owner password for USB device & emergency contact info
404
select part(s) of Electronic Health Record data to encrypt/protect
405
no
EHR includes unrestricted part?
406
yes
create 1st random password store in USB device
407
create 2nd random password send to server with unique ID
408
update database of unique IDs and respective encryption keys at server
409
encrypt 2nd random password with owner password, store in USB & computer
410
encrypt Electronic Health Record data parts with 1st/2nd random passwords
411
read 1st random password from USB, 2nd random password from computer
412
decrypt Electronic Health Record data parts with 1st/2nd random passwords

Figure 4

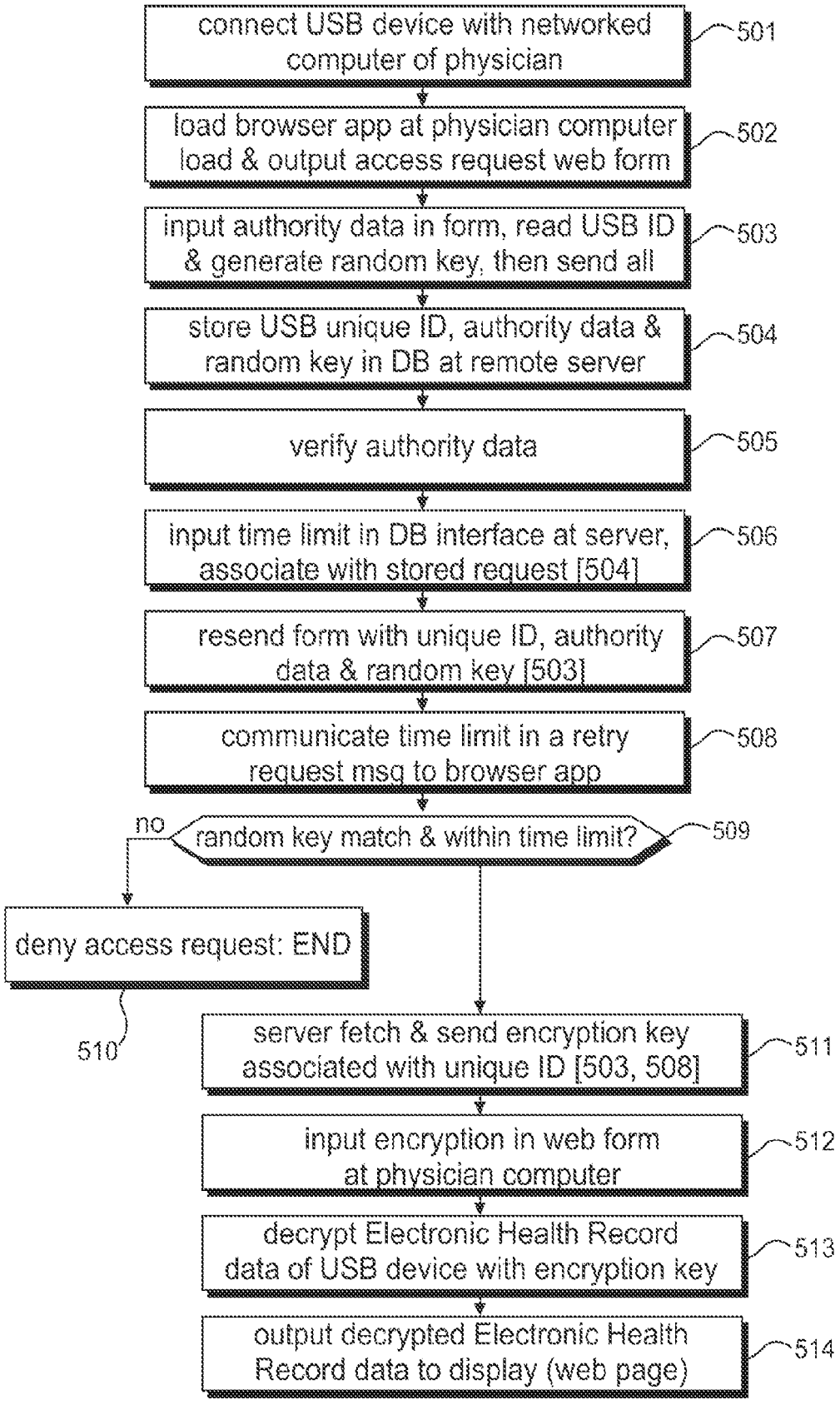
connect USB device with networked computer of physician
501
load browser app at physician computer load & output access request web form
502
input authority data in form, read USB ID & generate random key, then send all
503
store USB unique ID, authority data & random key in DB at remote server
504
verify authority data
505
input time limit in DB interface at server, associate with stored request [504]
506
resend form with unique ID, authority data & random key [503]
507
communicate time limit in a retry request msg to browser app
508
random key match & within time limit?
509
no
deny access request: END
510
server fetch & send encryption key associated with unique ID [503, 508]
511
input encryption in web form at physician computer
512
decrypt Electronic Health Record data of USB device with encryption key
513
output decrypted Electronic Health Record data to display (web page)
514

Figure 5

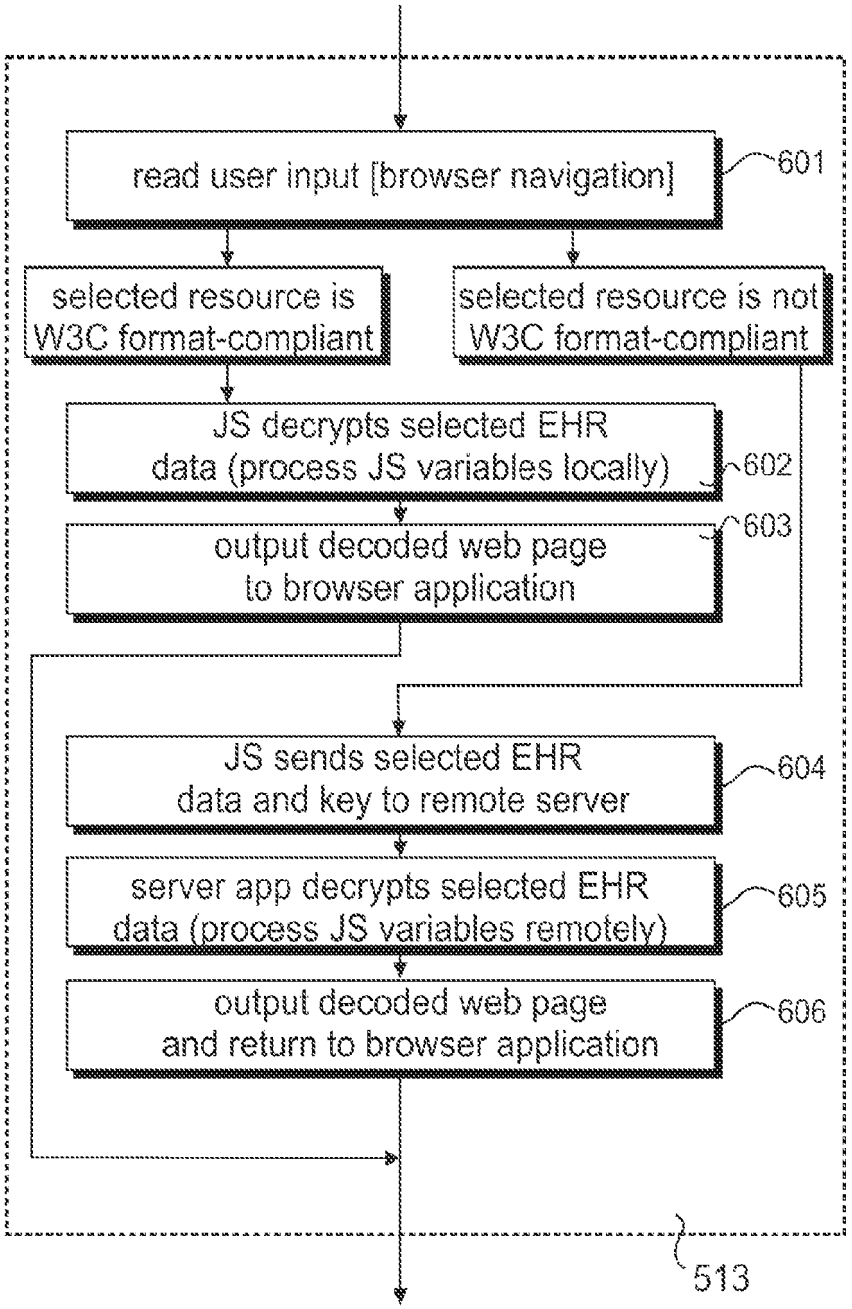
read user input [browser navigation]
601
selected resource is W3C format-compliant
selected resource is not W3C format-compliant
JS decrypts selected EHR data (process JS variables locally)
602
output decoded web page to browser application
603
JS sends selected EHR data and key to remote server
604
server app decrypts selected EHR data (process JS variables remotely)
605
output decoded web page and return to browser application
606
513

Figure 6

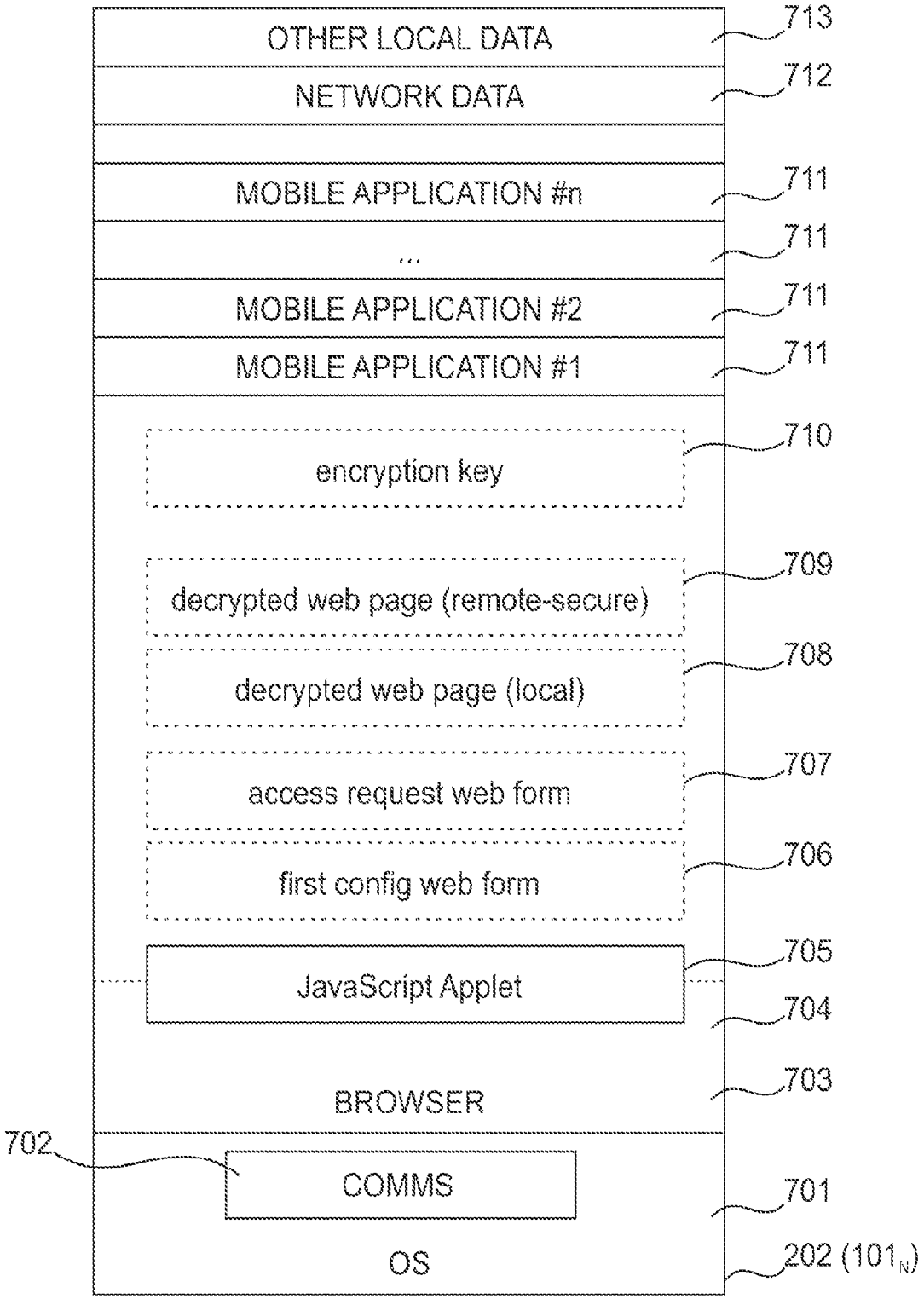
OTHER LOCAL DATA
713
NETWORK DATA
712
MOBILE APPLICATION #n
711
...
711
MOBILE APPLICATION #2
711
MOBILE APPLICATION #1
711
encryption key
710
decrypted web page (remote-secure)
709
decrypted web page (local)
708
access request web form
707
first config web form
706
JavaScript Applet
705
704
BROWSER
703
702
COMMS
701
OS
202 (101N)

Figure 7

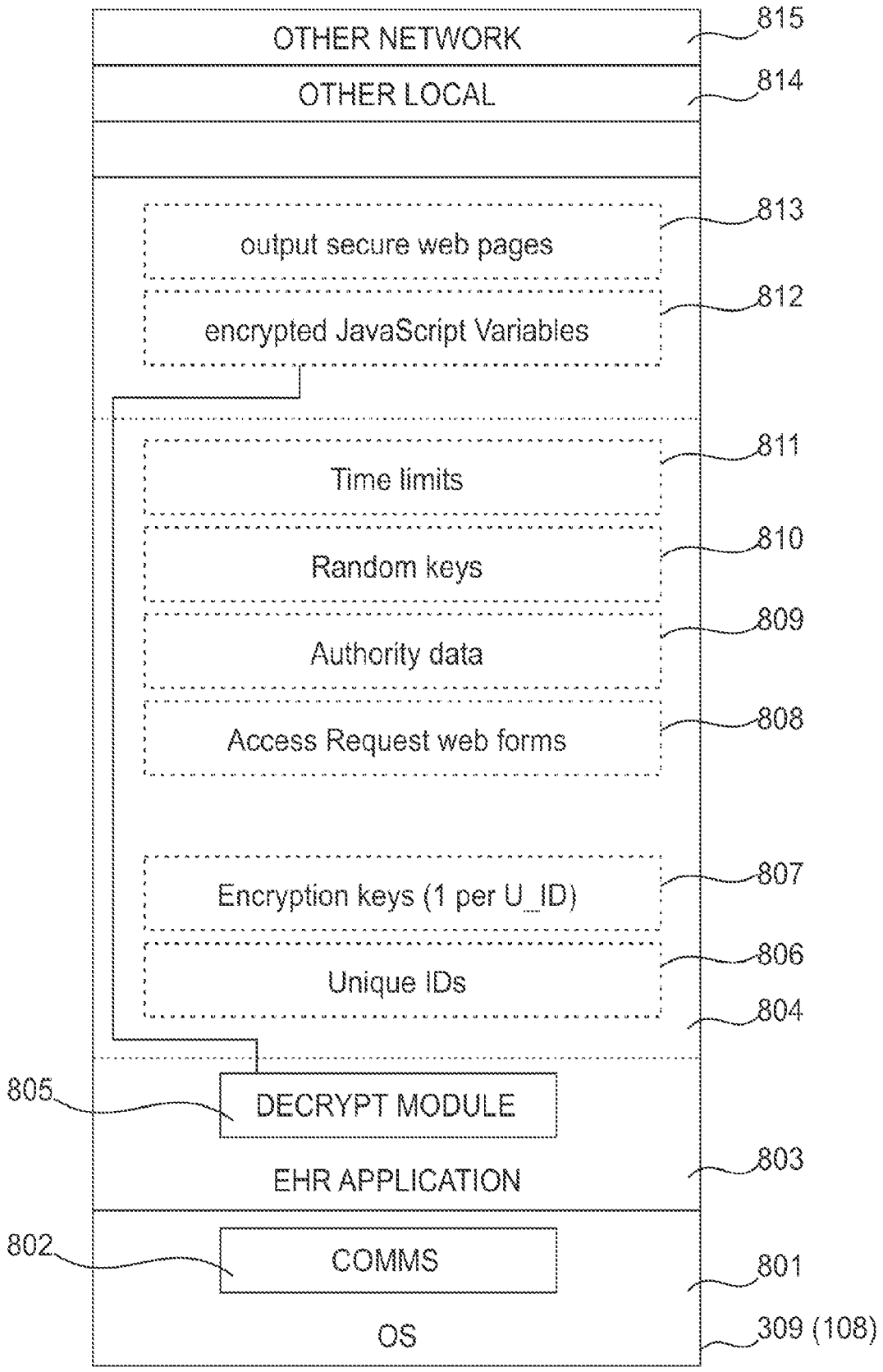
OTHER NETWORK
815
OTHER LOCAL
814
output secure web pages
813
encrypted JavaScript Variables
812
Time limits
811
Random keys
810
Authority data
809
Access Request web forms
808
Encryption keys (1 per U_ID)
807
Unique IDs
806
804
805
DECRYPT MODULE
EHR APPLICATION
803
802
COMMS
801
OS
309 (108)

Figure 8

METHOD AND SYSTEM FOR DISTRIBUTING HEALTH DATA

Field of the Invention

[0001] The present invention relates to a method and system for distributing health data. More particularly, the present invention is concerned with securely accessing patient or health data of an individual when emergency healthcare is required.

Background of the Invention

[0002] Many countries do not have centralised electronic health records and, in an emergency, or out-of-hours, or even at a scheduled appointment, an attending physician or health professional may not have all the information required about a patient available in a local data system, or from a remote data source, or supplied by the patient, particularly if the patient is incapacitated.

[0003] Patient health data is particularly sensitive and should only ever be consulted on an as-needed basis by a physician or emergency health professional. Therefore, the requirement of physical accessibility to such information, which may be satisfied by using a storage device with a generic interface such as USB, is at all times mitigated by the requirement of restricting access to such information to authorised persons only, which may be satisfied with a proprietary data format and/or password-based access restriction. This last solution is problematic if the patient is, at the material time, not in a condition to assess the authority of the access requester or to supply the password.

[0004] Some systems are known, wherein an individual or their physician input health data, or extract same from a practitioner database or the like, and store same in a data structure having a proprietary format on a removable data storage device, typically a flash memory stick. The memory stick also stores an executable program for executing by the data processing terminal of an attending health professional, in order to retrieve and display the health data. Distinct disadvantages of this approach are the potential incompatibility between the operating system of the data processing terminal and the executable program

and, frequently, network and/or system security measures which inhibit the local executing of the program.

[0005] An improved method of distributing and accessing health data of an individual is therefore required, and a system embodying this method, which mitigate at least the above shortcomings of the prior art.

Summary of the Invention

[0006] The present invention provides a distributed method and system, wherein patient health data is stored in encrypted, platform–agnostic format in a portable computer–readable medium with a generic terminal interface, and wherein the device further stores platform–agnostic means to request and obtain relevant decryption information from a remote server. The portable data storage device is carried by an individual whereby, should any health treatment be required, an attending health professional retrieves the medium from the individual and may consult personal health data thereon, by subjecting its decryption to a remote authorisation procedure. This solution advantageously overcomes any issue of actual or potential incompatibility between the terminal of a physician or health professional and/or its operating system, and the file system of the portable data storage device.

[0007] According to an aspect of the present invention, there is therefore provided a method of distributing health data, comprising at least one portable computer–readable medium, a server connected to a network and at least one computing device connected to the network, the method comprising the steps of storing encrypted health data of an individual and decryption means in a respective medium, the medium having a unique identifier and a respective encryption key; storing the or each unique identifier and the or each respective encryption key in the server; and, when the medium is read by the computing device connected to the network for accessing the encrypted health data stored therein, obtaining an authorization token from the server with the decryption means; obtaining the respective encryption key of the medium from the server

with the decryption means based on the authorization token; and decrypting the encrypted health data with the respective encryption key.

[0008] In an embodiment of the method according to the invention, the method may comprise the further step of generating the respective encryption key based on the unique identifier and a password for the medium.

[0009] In an embodiment of the method according to the invention, the step of obtaining an authorization token preferably comprises the further step of sending a first access request with the unique identifier of the medium and a random key to the server.

[00010] In another variant of these embodiments, the step of obtaining the respective encryption key preferably comprises the further step of sending a second access request to the server with the random key.

[00011] In an embodiment of the method according to the invention, the method may comprise the further step of associating a time limit with the authorization token. A variant of this embodiment may comprise the further step of sending the second access request within the time limit.

[00012] In an embodiment of the method according to the invention, the step of decrypting may comprise the further step of inputting the respective encryption key obtained from the server in the web form.

[00013] In an embodiment of the method according to the invention, the method may comprise the further step of subjecting the reading of the medium to inputting the password.

[00014] According to another aspect of the present invention, there is also provided a distributed health record system, comprising at least one portable computer–readable medium configured to store encrypted health data of an individual and decryption means, the or each medium having a unique identifier

and a respective encryption key; and a server connected to a network and configured to store the or each unique identifier and the or each respective encryption key; wherein, when the medium is read by a computing device connected to the network for accessing the encrypted health data stored therein, the decryption means configures the computing device to obtain an authorization token, then the respective encryption key of the medium, from the server.

[00015] In an embodiment of the system according to the invention, the decryption means may further configure the computing device to generate the respective encryption key based on the unique identifier and a password for the medium.

[00016] In a variant of these embodiments, the decryption means may further configure the computing device to send a first access request with the unique identifier of the medium to the server, for obtaining the authorization token.

[00017] In a variant of this embodiment, the decryption means may further configure the computing device to send a second access request to the server with the authorization token, for obtaining the respective encryption key of the medium.

[00018] In a variant of this further embodiment, the server is preferably configured to associate a time limit with the authorization token for sending the second access request. The server is preferably configured to deny the respective encryption key of the medium to the device when the second access request is sent after the time limit.

[00019] In an embodiment of the system according to the invention, access to the medium by the computing device for reading data stored therein is conditional upon inputting a password for the medium.

[00020] In an embodiment of the system according to the invention, the decryption means may configure the computing device to communicate with the server across the network via a HTML form.

[00021] According to yet another aspect of the present invention, there is also provided a set of instructions recorded on a portable computer–readable medium storing encrypted health data of an individual and having a unique identifier and a respective encryption key, wherein the set of instructions, when processed by a data processing terminal having networking means and accessing the medium for reading the encrypted health data, configures the terminal to obtain an authorization token from a remote server storing the unique identifier and the respective encryption key; obtain the respective encryption key of the medium from the server based on the authorization token; and decrypt the encrypted health data with the respective encryption key obtained.

[00022] The set of instructions is preferably embodied as a JavaScript applet for executing with a browser application, to facilitate the portability of the present solution to all computing devices regardless of their operating system and browser. Alternatively, the set of instructions may be embodied as any other client-side script, using any of Microsoft™ ActiveX™, Adobe™ Flash™ and the like.

[00023] For any of the above embodiments and further variants, the portable computer–readable medium may be selected from the group comprising random access memory devices, non-volatile random access memory devices, flash memory devices, electrically–erasable programmable read-only memory devices, optical data storage devices, magnetic data storage devices and networked data storage arrays and portions thereof.

[00024] For any of the above embodiments and further variants, the computing device in network communication with the server may selected from the group comprising computers, portable computers, tablet computers, mobile telephone handsets.

[00025] Other aspects are as set out in the claims herein.

Brief Description of the Drawings

[00026] For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

[00027] Figure 1 shows a network environment comprising a plurality of communication networks, a portable computer–readable medium carried by an individual in need of medical attention, a variety of computing devices that may be operated by an attending physician, and a remote server.

[00028] Figure 2 is a logical diagram of a typical hardware architecture of a mobile computing device shown in Figure 1, including memory means.

[00029] Figure 3 is a logical diagram of a typical hardware architecture of the server and a desktop computing device both shown in Figure 1, including memory means.

[00030] Figure 4 details the data processing steps of a method performed in the environment of Figure 1 for a first configuration of the portable computer–readable medium, including steps of encrypting and storing health data of an individual therein.

[00031] Figure 5 details the data processing steps of a method performed in the environment of Figure 1 for accessing encrypted health data of an individual stored in the portable computer–readable medium in an emergency, including steps of obtaining an authorization token and a respective encryption key from the server shown in Figures 1 and 3, and decrypting the encrypted health data at the mobile communication device shown in Figures 1 and 2.

[00032] Figure 6 further details an embodiment of the step of decrypting the encrypted health data.

[00033] Figure 7 is a logical diagram of the contents of the memory means of the server shown in Figures 1 and 3, when performing the method of Figures 5 and 6.

[00034] Figure 8 is a logical diagram of the contents of the memory means of the mobile communication device shown in Figures 1 and 2, when performing the method of Figures 4 to 6.

Detailed Description of the Embodiments

[00035] There will now be described by way of example a specific mode contemplated by the inventors. In the following description numerous specific details are set forth in order to provide a thorough understanding. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the description.

[00036] With reference to Figures 1 to 3, an example embodiment of a system according to the invention is shown within a networked environment. An individual 10 is equipped with a portable computer–readable medium 20, in the example a flash memory storage device 20 with a Universal Serial Bus (USB) interface 21. It will be readily understood by the skilled person from the foregoing, that the USB device 20 is provided herein by way of example only, and that it may be functionally substituted with any other random access memory device, non-volatile random access memory device, flash memory device, electrically–erasable programmable read-only memory device, optical data storage device such as a re-writable CD, magnetic data storage device such as a floppy disk or data card, and a networked data storage array or a portion thereof such as a distributed 'cloud' storage account.

[00037] The portable flash memory storage device 20 comprises a unique identifier 22, which is written to the medium at time of its initial configuration for use with the system of the invention. The portable flash memory storage device 20 stores health data of the individual 10 in encrypted form and at least one further data structure, as will be described hereafter.

[00038] A physician 30 is equipped with at least one computing device 101 selected from the group comprising a mobile telephone handset 101, a desktop computer 101 and a tablet computer 101. It will be appreciated in the context of the present invention that the physician should be interpreted broadly and to include a doctor, consultant or any health professional authorised to access or use the system of the present invention.

[00039] The mobile telephone handset 101 has wireless telecommunication emitting and receiving functionality over a cellular telephone network 100 configured according to the International Mobile Telecommunications-2000 (IMT — 2000, 'W-CDMA' or '3G') network industry standard, and wherein telecommunication is performed as voice, alphanumeric or audio-video data using the Short Message Service ('SMS') protocol, the Wireless Application protocol ('WAP') the Hypertext Transfer Protocol ('HTTP') or the Secure Hypertext Transfer Protocol ('HTTPS'). The handset 101 is preferably that commonly referred to as a 'smartphone' and may for instance be an iPhone™ handset manufactured by the Apple Corporation or a Nexus One™ handset manufactured for Google, Inc. by the HTC Corporation.

[00040] The mobile telephone handset 101 receives or emits voice, text, audio and/or image data encoded as a digital signal over a wireless data transmission 102, wherein the signal is relayed respectively to or from the handset by the geographically-closest communication link relay 103 of a plurality thereof. The plurality of communication link relays 103 allows digital signals to be routed between the handset 101, as it is geographically displaced in use, and its communication target(s) by means of a remote gateway 104 via a MSC or base

station 105. The gateway 104 is for instance a communication network switch, which couples digital signal traffic between wireless telecommunication networks, such as the cellular network 100 within which wireless data transmissions 102 take place, and another network 106 with a different protocol or topography, for instance a Wide Area Network ('WAN') such as the Internet 106. Accordingly, the gateway 104 further provides protocol conversion if required, for instance whether a handset 101 uses the WAP or HTTPS protocol to communicate data.

[00041] Alternatively, or additionally, the computing device 101 of the physician 30 may have wired and/or wireless telecommunication emitting and receiving functionality over, respectively, a wired local area network ('LAN') conforming to the IEEE 802.3 ('Gigabit Ethernet') standard or a wireless local area network ('WLAN') conforming to the 802.11 standard ('Wi-Fi'). In the LAN or WLAN, telecommunication is likewise performed as voice, alphanumeric and/or audio-video data using the Internet Protocol (IP), Voice data over IP ('VoIP') protocol, Hypertext Transfer Protocol ('HTTP') or Secure Hypertext Transfer Protocol ('HTTPS'), the signal being relayed respectively to or from the data processing device 101 by a wired (LAN) or wireless (WLAN) router 107 interfacing the mobile data communication device 101 to the WAN communication network 106.

[00042] Generally, the computing device 101 may be any stationary or portable data processing device having at least data processing means, data display means, wired and/or wireless communication means and an interface means suitable for accommodating the corresponding interface of the portable computer-readable medium 20, thus a corresponding USB socket in the example. It will therefore be readily understood by the skilled person from the present disclosure, that the physician computing device 101 may instead be a 'desktop' computer, a portable computer commonly referred to as a 'laptop' or 'netbook', a tablet computer such as an Apple™ iPad™ or a Motorola™ XOOM™, a personal digital assistant such as an Hewlett-Packard™ iPaq™, and the like.

[00043] A typical hardware architecture of the mobile telephone handset 101 of the example is shown in Figure 2 in further detail, by way of non-limitative example. The handset 101 firstly includes a data processing unit 201, for instance a general-purpose microprocessor ('CPU'), acting as the main controller of the handset 101 and which is coupled with memory means 202, comprising non-volatile random-access memory ('NVRAM').

[00044] The mobile telephone handset 101 further includes a modem 203 to implement the wireless communication functionality, as the modem provides the hardware interface to external communication systems, such as the closest communication link relay 103 and ensuing cellular telephone network 104, 105 shown in Figure 1. An aerial 204 coupled with the modem 203 facilitates the reception of wireless signals from nearby communication link relays 103. The modem 203 is interfaced with, or includes, an analogue-to-digital converter ('ADC') 205 for demodulating wavelength wireless signals received via the antenna 204 into digital data, and reciprocally for outgoing data.

[00045] The handset 101 further includes self-locating means in the form of a GPS receiver 206, wherein the ADC 205 receives analogue positional and time data from orbiting satellites (not shown), which the data processing unit 201 or a dedicated data processing unit processes into digital positional and time data.

[00046] The handset 101 further includes a sound transducer 207, for converting ambient sound waves, such as the user's voice, into an analogue signal, which the ADC 205 receives for the data processing unit 201 or a dedicated data processing unit to process into digital audio data.

[00047] The handset 105 further includes imaging means 208 in the form of an electronic image sensor, for capturing image data which the data processing unit 201 or a dedicated data processing unit processes into digital image data.

[00048] The CPU 201, NVRAM 202, modem 203, GPS receiver 206, microphone 207 and digital camera 208 are connected by a data input/output bus

209, over which they communicate and to which further components of the handset 101 are similarly connected, in order to provide wireless communication functionality and receive user interrupts, inputs and configuration data.

[00049] Alphanumerical and/or image data processed by CPU 201 is output to a video display unit 210 ('VDU'), from which user interrupts may also be received if it is a touch screen display. Further user interrupts may also be received from a keypad 211 of the handset or from an external human interface device ('HiD') connected to the handset via a Universal Serial Bus ('USB') interface 212. The USB interface advantageously also allows the CPU 201 to read data from and/or write data to the removable storage device 20. Audio data processed by CPU 201 is output to a speaker unit 213.

[00050] Power is provided to the handset 101 by an internal module battery 214, which an electrical converter 215 charges from a mains power supply as and when required.

[00051] The networked environment next includes at least one data processing terminal 108 configured as a server for use with the system of the present invention. The server 108 emits and receives data encoded as a digital signal over a wired data transmission conforming to the IEEE 802.3 ('Gigabit Ethernet') standard, wherein the signal is relayed respectively to or from the computing device by a wired router 107 interfacing the server 108 to the WAN communication network 106. Generally, the server 108 may be any portable or desktop data processing device having networking means apt to establish a data communication with any one data communication device 101.

[00052] A typical hardware architecture of the data processing terminal 108 is now shown in Figure 3 in further detail, by way of non-limitative example. The data processing device 108 is a computer configured with a data processing unit 301, data outputting means such as video display unit (VDU) 302, data inputting means such as HiD devices, commonly a keyboard 303 and a pointing device (mouse) 304, as well as the VDU 302 itself if it is a touch screen display, and

data inputting/outputting means such as a wired network connection 305 to the communication network 106 via the router 107, a magnetic data-carrying medium reader/writer 306 and an optical data-carrying medium reader/writer 307.

[00053] Within data processing unit 301, a central processing unit (CPU) 308 provides task co-ordination and data processing functionality. Sets of instructions and data for the CPU 308 are stored in memory means 309 and a hard disk storage unit 310 facilitates non-volatile storage of the instructions and the data. A network interface card (NIC) 311 provides the interface to the network connection 305. A universal serial bus (USB) input/output interface 312 facilitates connection to the keyboard and pointing devices 303, 304.

[00054] All of the above components are connected to a data input/output bus 313, to which the magnetic data-carrying medium reader/writer 306 and optical data-carrying medium reader/writer 307 are also connected. A video adapter 314 receives CPU instructions over the bus 313 for outputting processed data to VDU 302. All the components of data processing unit 301 are powered by a power supply unit 315, which receives electrical power from a local mains power source and transforms same according to component ratings and requirements.

[00055] Details of the data processing steps of a method for first configuring the USB device 20, as performed in the environment of Figure 1, are explained hereafter with reference to Figure 4. Before they are released to respective individuals, or to physicians for redistribution, all portable computer-readable media 20 for use with the method are initially configured once-only at step 401, with a unique identifier 22, for instance a respective serial number, which is stored therein in a format readable by a browser application, and which is also stored by the server 108 in unencrypted form in a database.

[00056] After they are released to respective individuals or physicians, and at any first visit of an individual to their physician or other health professional with access to an Electronic Health Record data source, each portable computer-

readable medium 20 is interfaced with the physician's computing device at step 402. In the example, the USB device 20 is interfaced with the USB port 312 of the local computing device 101 of the physician, and a local set of instructions extracts the Electronic Health Record data of the individual from one or more conventional Practice Management Database systems,

[00057] At step 403, the set of instructions converts the retrieved Electronic Health Record data into a file or series of files readable by most web browsers in a W3C-compliant standardised display format, including non-standard data and files, particularly document-type data such as scanned files, written reports, letters, ECGs and the like, as described hereinbelow. In a preferred embodiment, the retrieved Electronic Health Record data is converted into a standardised series of linked HTML pages, each such page storing specific Electronic Health Record information.

[00058] At step 404, the set of instructions outputs a web form or the like to the VDU 302 of the computing device 101 and causes the individual to provide and input a respective password, as well as emergency contact information, then to select which elements, parts and/or features of their individual Electronic Health Record data to encrypt at step 405.

[00059] The set of instructions is configured to allow partial selection of elements, parts and/or features of the individual Electronic Health Record data, thus all or part of the individual Electronic Health Record data may remain unencrypted.

[00060] Accordingly, a question is asked at step 406, as to whether any part of the Electronic Health Record data record is to be available without the user password or authentication. If the question is answered positively, then at step 407, a first random password is created and stored on the USB stick.

[00061] When the question of step 406 is answered negatively, or upon completing step 407, then at step 408 a second random password is created and

sent to the remote server 108 along with the unique identifier 22 read from the USB device 20 by the set of instructions, in respect of any part of the Electronic Health Record data record that is to be available only with the user password or authentication.

[00062] The server 108 stores a database of unique identifiers 22 for all issued USB devices 20 and their respective encryption keys once configured and communicated according to step 401 to 408 whereby, upon receiving the communication of step 408, at step 409 the server 108 updates the database by matching the communicated device unique identifier 22 against its equivalent in the database, then storing the communicated respective encryption key against same therein.

[00063] At step 410, the second random password is encrypted with the password input by the individual, and stored encrypted in the USB device 20 and unencrypted in the local computing device 101 of the physician, in respect of future visits by the individual for updating the Electronic Health Record data. It will be appreciated that USB key is encrypted while computer key is not encrypted.

[00064] At step 411, the Electronic Health Record HTML data of step 402 is encrypted, with the first random password as the encryption key for those parts of the data that are to be available without the user password or authentication and, respectively, with the second random password as the encryption key for those parts of the data that are to be available only with the user password or authentication. At step 412, the encrypted Electronic Health Record HTML data is stored in the USB device 20.

[00065] On any next visit of that physician by that individual, the encrypted Electronic Health Record HTML data may be retrieved and decrypted for perusing and/or updating same, by interfacing the USB device 20 is interfaced with the USB port 312 of the local computing device 101 of the physician per step 402 then, at step 412, retrieving either or both of the first random password from the USB device 20 pursuant to step 407 and the second random password from

the local computing device 101 pursuant to step 410, as required by the encryption choices of the individual at step 405.

[00066] The portable device 20 at this time is thus configured with the encrypted Electronic Health Record data of the visiting individual, a platform-agnostic program to encrypt and decrypt same, and the respective encryption key used by the platform-agnostic program for the encrypting and decrypting tasks. The encrypted Electronic Health Record data thus remains at all times in the sole control of the individual, since the physician device 101 does not store the individual password, nor the unique identifier 22 of the USB device 20, nor the respective encryption key; and since the server 108 does not store the Electronic Health Record data, encrypted or otherwise.

[00067] Details of the data processing steps of a method as performed in the environment of Figure 1, for accessing the encrypted health data of an individual stored in the USB device 20, are explained hereafter with reference to Figure 5. Reasons for accessing the encrypted health data may be varied. For instance an individual carrying a USB device 20 suitably configured according to steps 401 to 411 may become in need of emergency medical care, and even be unconscious, thus unable to inform any attending physician or emergency healthcare provider about any medical condition, allergies and the like that can prove critical to the care provided; alternatively, the individual may be visiting a consultant for a specialist health check , pursuant to a referral from their physician with whom the USB device 20 was first configured according to steps 401 to 411.

[00068] Accordingly, the USB device 20 is retrieved from the individual and, at step 501, the USB device 20 is again interfaced with the USB port 212 of a local computing device 101. The device is read by the operating system of the computing device 101 and, at step 502, the platform-agnostic program autoruns and causes a browser application of the local device 101 to execute, or the executing of the browser can be initiated by the operator, and then to load and output a web form to the display 210 as before. However, there is now an

encryption key stored in the USB device 20 and the web form of step 502 is now a data access request which requires information identifying the requesting physician, the place of healthcare provision and the like, at least sufficient to verify the authority vesting in the requester, when the individual is unable to provide their access password.

[00069] Correspondingly, at step 503, the attending physician the identifying information, in the web form. Once completed, the platform-agnostic program reads the unique identifier 22 from the USB device 20 and generates a random key, then submits the form to the server 108 with the random key and the unique identifier 22 over the network 106. The server 108 receives the complete web form data as a health record access request, together with the random key, and stores both in a database at step 504. The random key is stored therein as an authorization token, since it will be compared for identity against a second request from the physician device 101 described hereafter, in order to authorise release of the encryption key for decrypting the health data stored on the USB device 20.

[00070] A user of the server 108 subsequently verifies the accuracy of the identifying information at step 505, via relevant, conventional means outside the scope of the present disclosure. When the identifying information has been verified as accurate, the user of the server 108 inputs a time limit in a relevant interface of the database displayed on the VDU 302 of the server 108 at step 506. The time limit is associated with the health record access request and the random key, stored therewith in the database, and the server communicates the time limit in response to a retry request message to the platform-agnostic program at the physician terminal 101 over the network 106 at step 507. The terminal 101 receives the reply to its retry request message from the server 108 and, at step 508, the platform-agnostic program resubmits the form to the server 108 with the random key.

[00071] A question is next asked at the server at step 509, as to whether the random key in the resubmitted form matches the random key stored in the

database at step 504, and whether the form has been resubmitted within the time limit stored in the database at step 506. If either of the two parameters does not match, the question is answered negatively and the access request from the physician terminal 101 is denied at step 510. However, if both parameters match, the question is answered positively and, at step 511, the server 108 retrieves the encryption key respectively associated with the unique identifier 22 of step 503 from the database, and communicates it to the web form interface of the platform-agnostic program at the physician terminal 101. At step 512, the physician may copy-type the communicated encryption key in the same or another web form of the platform-agnostic program, for decrypting the encrypted Electronic Health Record data locally at step 513 and outputting same to the display 210 at step 514.

[00072] Details of the data processing steps of an embodiment of step 513 for decrypting the encrypted Electronic Health Record data stored in the USB device 20 , as performed in the environment of Figure 1, are explained hereafter with reference to Figure 6. To display decrypted Electronic Health Record data at step 514, HTML pages are created from the Electronic Health Record data at step 410. These pages are encrypted with the AES encryption algorithm and stored as JavaScript variables in Hex as part of an HTML page during step 410. It will be readily understood by the skilled reader that many other encryption algorithms, known and yet to be devised, may be used to perform the above encryption, and that encrypted pages may be stored according to any one of a variety of ASCII encoding schemes, for instance Base64.

[00073] Pseudo-source code for such an HTML page is provided herein by way of example, as follows:

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<script language="JavaScript" type="text/javascript" src="../CompleteGP.js"></script>
<script language="JavaScript" type="text/javascript" src="../Decrypt.js"></script>
<script type="text/javascript" language="JavaScript">
<!--
var
Data='2923BE84E16CD6AE529049F1F1BBE9EBCA1DB444FC1F5827FCA7C552B97ED6
4AA3BDFD442F27029E'+
```

```
(lines removed for not obscuring the description unnecessarily)

'B5565DCF51E857AC593F5E53F268A8BB0A198AD07DAD36D8F2101A1EF84B856DD56
0C78C4402985F'+
'67449E5AFBC9122335E71ED98871F67BF33BFFA98FC7FD7B58DE2FA2311E54AAD6A
ADE6BF6C783C2'; Data = Data +
'3C3E5362E97A8C866DEBC0ACDC491BDFDDC94CED4A93CD29';
// -->
</script>
</head>
<body onload="DecodePage(Data,'C1');">
</body>
</html>
```

[00074] Accordingly, in use, at step 601 the browser application reads the user inputs provided by the physician to the terminal 101, typically navigational choices translated as the selection of hyperlinks embedded in the displayed web page or form, such hyperlinks pointing to discrete aspects of the encrypted Electronic Health Record data, i.e. JavaScript variables. The JavaScript applet in combination with the browser application decodes these variables with the communicated encryption key at step 602, and redirects the browser application to the decoded web page at step 603, whereby the decoded web page is output to the display 210 at step 514.

[00075] However, web browser applications do not routinely allow for the decryption and display of files in a format not complying with World Wide Web Consortium (WC3) standards, for instance scanned documents or files according to the Microsoft Word, Adobe PDF, RTF or DICOM formats. Such files are also encrypted (AES) and stored as JavaScript variables in Hex as part of an HTML page during step 410.

[00076] The server 108 is advantageously further configured to execute a program which decrypts encrypted document-type files and returns same to the terminal 101 as a standards-compliant web page. Accordingly, when the physician interacting with the browser application at the terminal 101 requires decryption of one such non-standard file at step 601, the JavaScript applet communicates the JavaScript variables which contain the file to the server 108 as a web form with the encryption key over a secure network connection at step 604. The program at the server 108 then decrypts the file with the communicated

key at step 605, and returns the decrypted result over the secure network connection to the browser application of the terminal 101 at step 606 as a new, standards-compliant web page, that can again be displayed by same at step 514. The file is never stored and always transmitted securely.

[00077] A logical diagram of the contents of the memory means 202 of the physician mobile communication device 101, when performing steps of a method of Figures 4 to 6 at runtime, is shown in Figure 7. An operating system is shown at 701 which, depending on the handset manufacturer, may be iOS 5™ developed and distributed by Apple Inc. or Android™ developed and distributed by Google Inc.

[00078] A communication subset 702 of the OS 801 receives and processes all incoming and outgoing signalling data, respectively to or form any application #1, #2, #3...#n stored at and processed as local data by the mobile communication device 101, including a browser application 703.

[00079] The platform-agnostic program is shown at 705, which configures the mobile communication device 101 to perform a method as described with reference to Figures 4 to 6, and which is interfaced with the OS 801, particularly the communication subset 802 thereof, via one or more suitable Application Programmer Interfaces. In the example, the program 705 is JavaScript applet which most browser applications can execute at runtime, irrespective of the operating system 801.

[00080] Data processed by the browser 702 and the applet 705 is shown generally at 704 and may comprise a first configuration web form 706 of step 403; an Electronic Health Record data access request web form 707 of steps 502, 508; one or more decrypted web pages 708 of steps 513, 514; one or more remotely-decrypted, secure web pages 709 of steps 605, 606; and an encryption key 710 of steps 405, 407, 410, 512, 513, 602, 604.

[00081] Network data shown at 712 and comprises incoming and outgoing network data, respectively for or from the browser 703 and the applet 705. The memory 202 may further comprise local data 713 that is unrelated to the browser 702 or the applet 705, for instance used by or generated for another application 711 being processed in parallel with the browser 703 and the applet 705, typically input data of the user or graphical data for the OS or application user interface.

[00082] A logical diagram of the contents of the memory means 309 of the server 108, when performing a method as described with reference to Figures 4 to 6 at runtime, is shown next in Figure 8. An operating system is shown at 801 which, if the server 108 is a desktop computer, is for instance Windows 8™ distributed by the Microsoft Corporation. The OS 801 includes communication subroutines 802 to configure the terminal for bilateral network communication via the NIC 311.

[00083] An application is shown at 803, which configures the server 108 to perform steps of the method according to the invention as described hereinbefore with reference to Figures 4 to 6, and which is interfaced with the OS 801 and network communication subroutines 802 thereof via one or more suitable Application Programmer Interfaces. In particular, the application 803 comprises a database 804 substantially as hereinbefore described, and a decrypting module 805 for performing steps 605 and 606.

[00084] The database 804 processed by the application 803 at runtime and likewise stored in the memory 309 includes unique identifiers 806 (22) of each issued USB device 20; their respective encryption key 807 (710) once configured according to steps 405 to 408; access request web forms 808 (707) received from step 503 for performing steps 504 to 509, including physician authority data 809 and random keys 810 retrieved from same and stored according to step 504; time limits 811 respectively associated with verified access request web forms 808 according to step 506.

[00085] The JavaScript variables input to the decrypting module 805 at step 604 for processing at step 604 are shown at 812 and are not included in the database data 804. Likewise, the decrypted web pages returned to the originating browser 703 at step 606 are shown at 813 and are again not included in the database data 804.

[00086] The memory 309 may further comprise local and/or network data that is unrelated to the application 803, respectively shown at 814 and 815, as used by or generated for another application being processed in parallel with the application 803, for instance by the user of the server 108 for verifying the physician authority data at step 505.

[00087] The embodiments in the invention described with reference to the drawings comprise a computer apparatus and/or processes performed in a computer apparatus. However, the invention also extends to computer programs, particularly computer programs stored on or in a carrier adapted to bring the invention into practice. The program may be in the form of source code, object code, or a code intermediate source and object code, such as in partially compiled form or in any other form suitable for use in the implementation of the method according to the invention. The carrier may comprise a storage medium such as ROM, e.g. CD ROM, or magnetic recording medium, e.g. a floppy disk or hard disk. The carrier may be an electrical or optical signal which may be transmitted via an electrical or an optical cable or by radio or other means.

[00088] In the specification the terms "comprise, comprises, comprised and comprising" or any variation thereof and the terms include, includes, included and including" or any variation thereof are considered to be totally interchangeable and they should all be afforded the widest possible interpretation and vice versa.

[00089] The invention is not limited to the embodiments hereinbefore described but may be varied in both construction and detail.

Claims

1. A method of distributing health data, comprising at least one portable computer–readable medium, a server connected to a network and at least one computing device connected to the network, the method comprising the steps of

storing encrypted health data of an individual and decryption means in a respective medium, the medium having a unique identifier and a respective encryption key;

storing the or each unique identifier and the or each respective encryption key in the server; and

when the medium is read by the computing device connected to the network for accessing the encrypted health data stored therein,

obtaining and storing an authorization token at the server from the decryption means;

obtaining the respective encryption key of the medium from the server with the decryption means based on the authorization token; and

decrypting the encrypted health data with the respective encryption key.

2. A method according to claim 1, comprising the further step of generating the respective encryption key based on the unique identifier and a password for the medium.

3. A method according to claim 1 or 2, wherein the step of obtaining an authorization token comprises the further step of sending a first access request with the unique identifier of the medium and a random key to the server.

4. A method according to claim 3, wherein the step of obtaining the respective encryption key comprises the further step of sending a second access request to the server with the random key.

5. A method according to any of claims 1 to 4, comprising the further step of associating a time limit with the authorization token.

6. A method according to claim 5, comprising the further step of sending the second access request within the time limit.

7. A method according to any of claims 4 to 6, wherein the step of decrypting comprises the further step of inputting the respective encryption key obtained from the server in the web form.

8. A method according to any of claims 2 to 7, comprising the further step of subjecting reading of the medium to inputting the password.

9. A method according to any of claims 1 to 8, wherein the at least one portable computer–readable medium is selected from the group comprising random access memory devices, non-volatile random access memory devices, flash memory devices, electrically–erasable programmable read-only memory devices, optical data storage devices, magnetic data storage devices and networked data storage arrays and portions thereof.

10. A distributed health record system, comprising

at least one portable computer–readable medium configured to store encrypted health data of an individual and decryption means, the or each medium having a unique identifier and a respective encryption key; and

a server connected to a network and configured to store the or each unique identifier and the or each respective encryption key;

wherein, when the medium is read by a computing device connected to the network for accessing the encrypted health data stored therein, the decryption means configures the computing device to obtain an authorization token, then the respective encryption key of the medium, from the server.

11. A system according to claim 10, wherein the decryption means further configures the computing device to generate the respective encryption key based on the unique identifier and a password for the medium.

12. A system according to claim 11, wherein the decryption means further configures the computing device to send a first access request with the unique identifier of the medium to the server, for obtaining the authorization token.

13. A system according to claim 12 wherein the decryption means further configures the computing device to send a second access request to the server with the authorization token, for obtaining the respective encryption key of the medium.

14. A system according to claim 13, wherein the server is configured to associate a time limit with the authorization token for sending the second access request.

15. A system according to claim 14, wherein the server is configured to deny the respective encryption key of the medium to the device when the second access request is sent after the time limit.

16. A system according to any of claims 11 to 15, wherein access to the medium by the computing device for reading data stored therein is conditional upon inputting the password.

17. A system according to any of claims 10 to 16, wherein the decryption means configures the computing device to communicate with the server across the network via a HTML form.

18. A system according to any of claims 10 to 17, wherein the at least one portable computer–readable medium is selected from the group comprising random access memory devices, non-volatile random access memory devices, flash memory devices, electrically–erasable programmable read-only memory devices, optical data storage devices, magnetic data storage devices and networked data storage arrays and portions thereof.

19. A system according to any of claims 10 to 18, wherein the computing device is selected from the group comprising computers, portable computers, tablet computers, mobile telephone handsets.

20. A set of instructions recorded on a data carrying medium storing encrypted health data of an individual and having a unique identifier and a respective encryption key, wherein the set of instructions, when processed by a data processing terminal having networking means and accessing the medium for reading the encrypted health data, configures the terminal to

obtain an authorization token from a remote server storing the unique identifier and the respective encryption key;

obtain the respective encryption key of the medium from the server based on the authorization token; and

decrypt the encrypted health data with the respective encryption key obtained.

21. A set of instructions according to claim 20, wherein the data carrying medium is selected from the group comprising random access memory devices, non-volatile random access memory devices, flash memory devices, electrically–erasable programmable read-only memory devices, optical data storage devices, magnetic data storage devices and networked data storage arrays and portions thereof.

22. A set of instructions may according to claim 20 or 21, embodied as one selected from the group comprising a JavaScript applet, an ActiveX control and a Flash applet, for executing with a browser application.

23. A method substantially as described herein, in association with and as shown in the accompanying drawings.

24. A system substantially as described herein, in association with and as shown in the accompanying drawings.

Application No: GB1222856.5 **Examiner:** Mr Ben Widdows

Claims searched: 1-9 **Date of search:** 18 July 2013

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1,2,5&7-9	US 2009/0055924 A1 (TROTTER) see whole document, esp. paragraphs 29,31,55&59
A	-	JP 2003296453 A (MATSUSHITA ELECTRIC) see abstract and figs
A	-	GB 2479074 A (VOLTAGE SECURITY INC) see abstract and fig 8

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G06F; G06Q

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC

International Classification:

Subclass	Subgroup	Valid From
G06F	0021/62	01/01/2013
G06Q	0050/24	01/01/2012