(12) UK Patent Application (19) GB (11) 2491220 (13) A

(43) Date of A Publication 28.11.2012

(21) Application No: 1201370.2

(22) Date of Filing: 27.01.2012

(30) Priority Data:
(31) 1108675 (32) 24.05.2011 (33) GB

(71) Applicant(s):
Bob Beatty
19 Benson Road, HENFIELD, Sussex, BN5 9HY, United Kingdom

Nick Evans
74 Shirley Street, HOVE, Sussex, BN3 3WG, United Kingdom

Addam Ltd
(Incorporated in the United Kingdom)
St Clears Farm, FLETCHING, Sussex, TN22 3YA, United Kingdom

(72) Inventor(s):
Bob Beatty
Nick Evans

(74) Agent and/or Address for Service:
Bob Beatty
19 Benson Road, HENFIELD, Sussex, BN5 9HY, United Kingdom

(51) INT CL:
G06K 19/06 (2006.01) ***G06K 7/14*** (2006.01)

(56) Documents Cited:
GB 2459686 A **US 20100219241 A1**
US 20060144946 A1
www.isavemylife.com

(58) Field of Search:
INT CL **G06K**
Other: **WPI, EPODOC**

(54) Title of the Invention: **System and method for holding and selectively retrieving information from a mobile device using a data matrix code**
Abstract Title: **Displaying and selectively retrieving information encoded in a data matrix**

(57) The method comprises encrypting data into a single data matrix image, such as a QR Code and allowing it to be decoded in such a way that different viewers can access different elements of the data, when it is being displayed on a mobile device such as a smart phone. An owner of the data first submits data through a program which encodes it as a data matrix image which is then displayed on the owner's mobile display device. Software running on a reader device 320 viewing the data matrix image 330 displays information from the image and if some fields are encrypted 350, may prompt the user to provide an unlock key. After the correct unlock key has been submitted by the user, the software may display the encrypted fields 350 as well as the unencrypted fields 340. The data matrix image, or 2D barcode, could contain medical or other personal data.

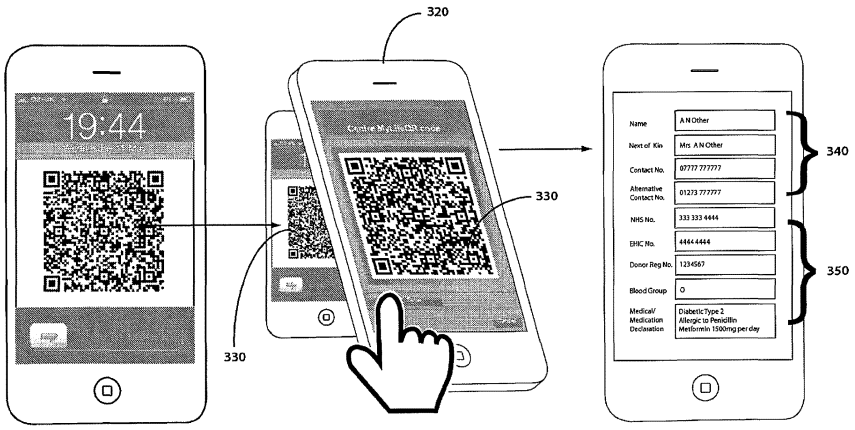

Fig.80

GB 2491220 A

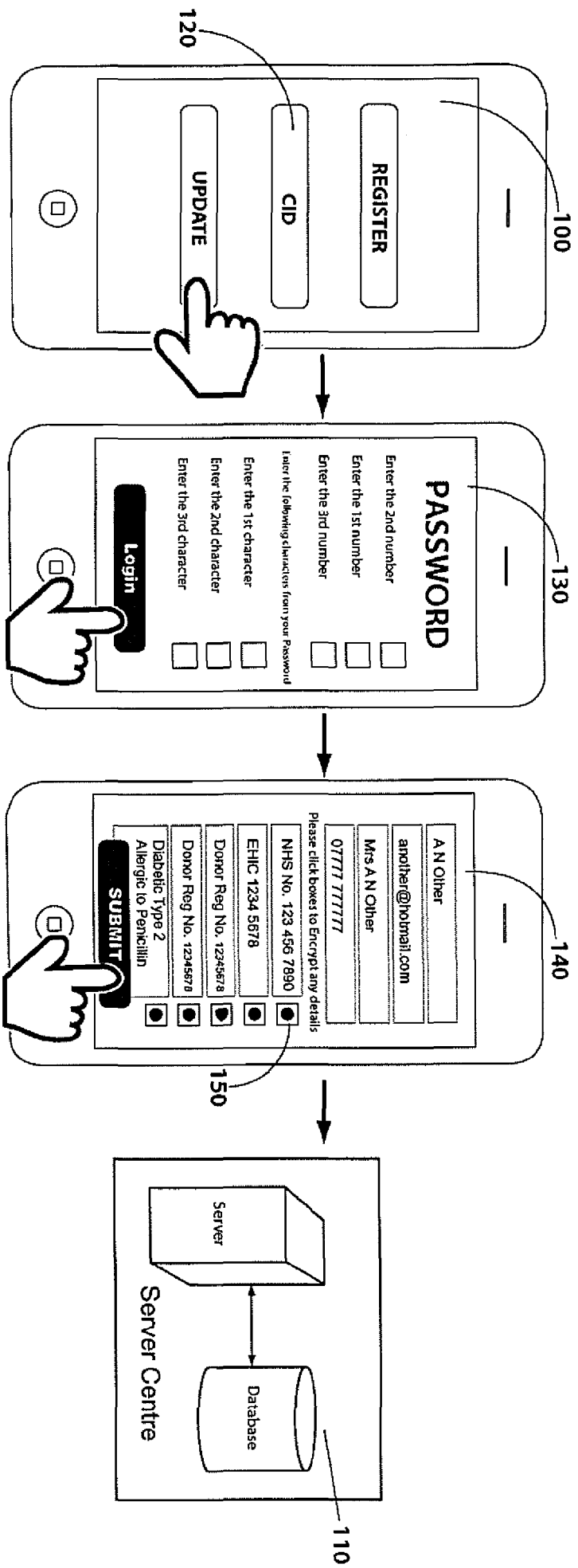
120
100
REGISTER
CID
UPDATE
130
PASSWORD
Enter the 2nd number
Enter the 1st number
Enter the 3rd number
Enter the following characters from your Password
Enter the 1st character
Enter the 2nd character
Enter the 3rd character
Login
140
A N Other
another@hotmail.com
Mrs A N Other
07777 777777
Please click boxes to Encrypt any details
NHS No. 123 456 7890
EHIC 1234 5678
Donor Reg No. 12345678
Donor Reg No. 12345678
Diabetic Type 2
Allergic to Penicillin
SUBMIT
150
Server
Server Centre
Database
110

Fig.10

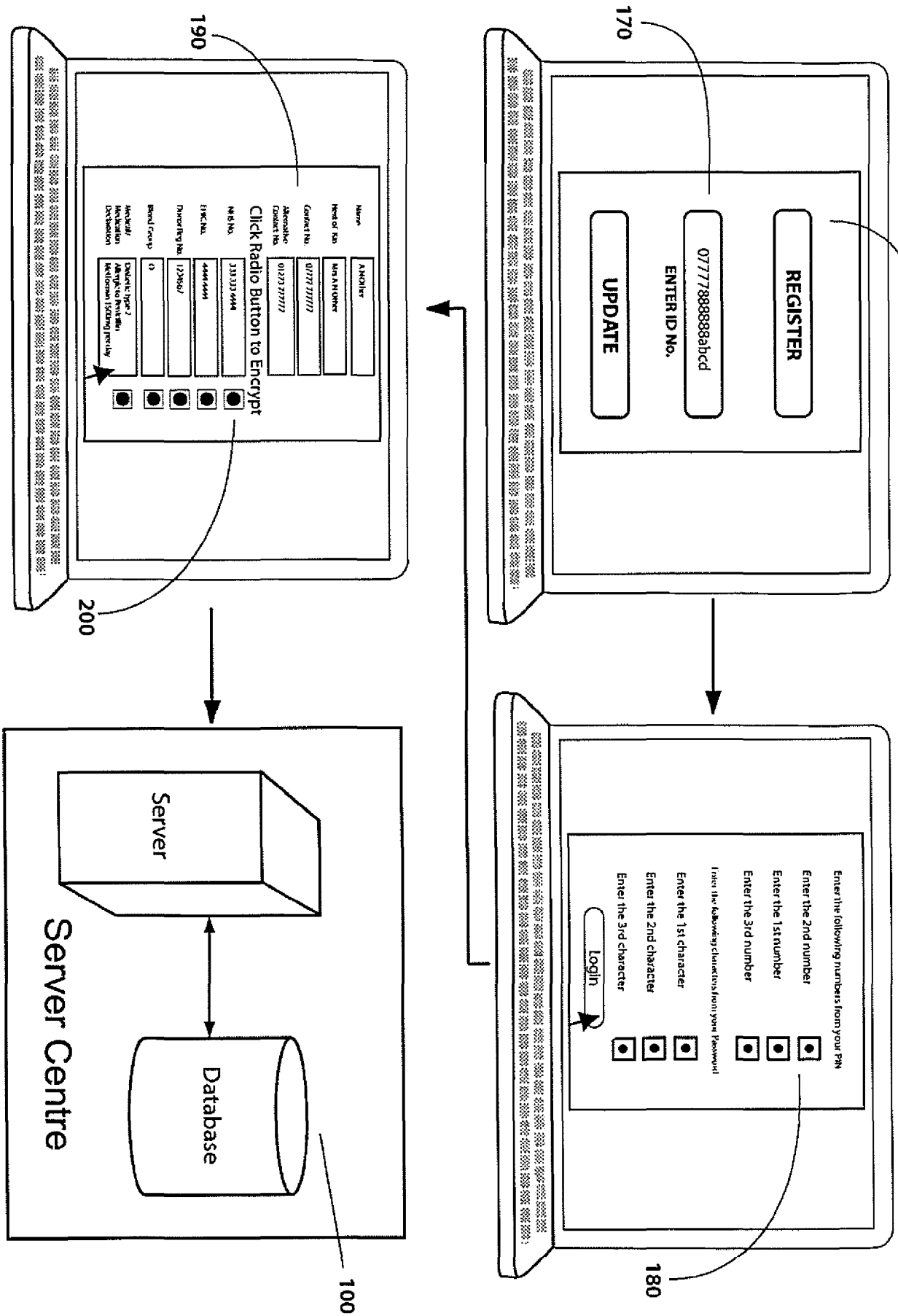
160
REGISTER
07777888888abcd
ENTER ID No.
UPDATE
170
190
Click Radio Button to Encrypt
200
180
Enter the following numbers from your PIN
Enter the 2nd number
Enter the 1st number
Enter the 3rd number
Enter the 1st character
Enter the 2nd character
Enter the 3rd character
Login
100
Server
Database
Server Centre

Fig.11

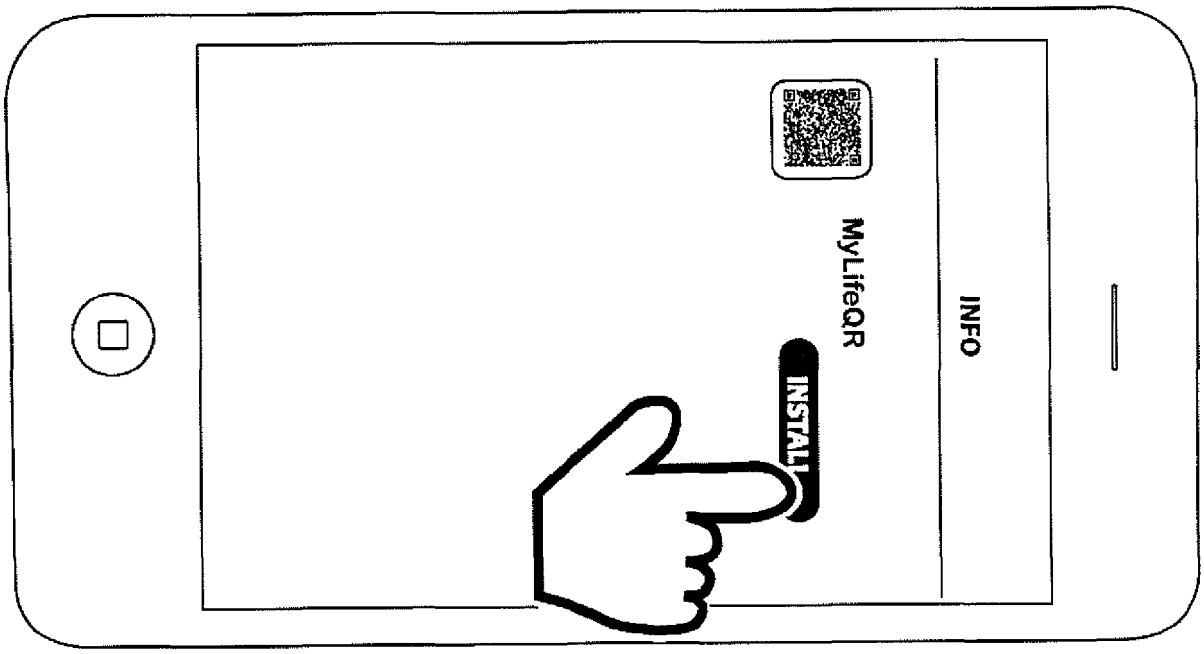

Fig.20

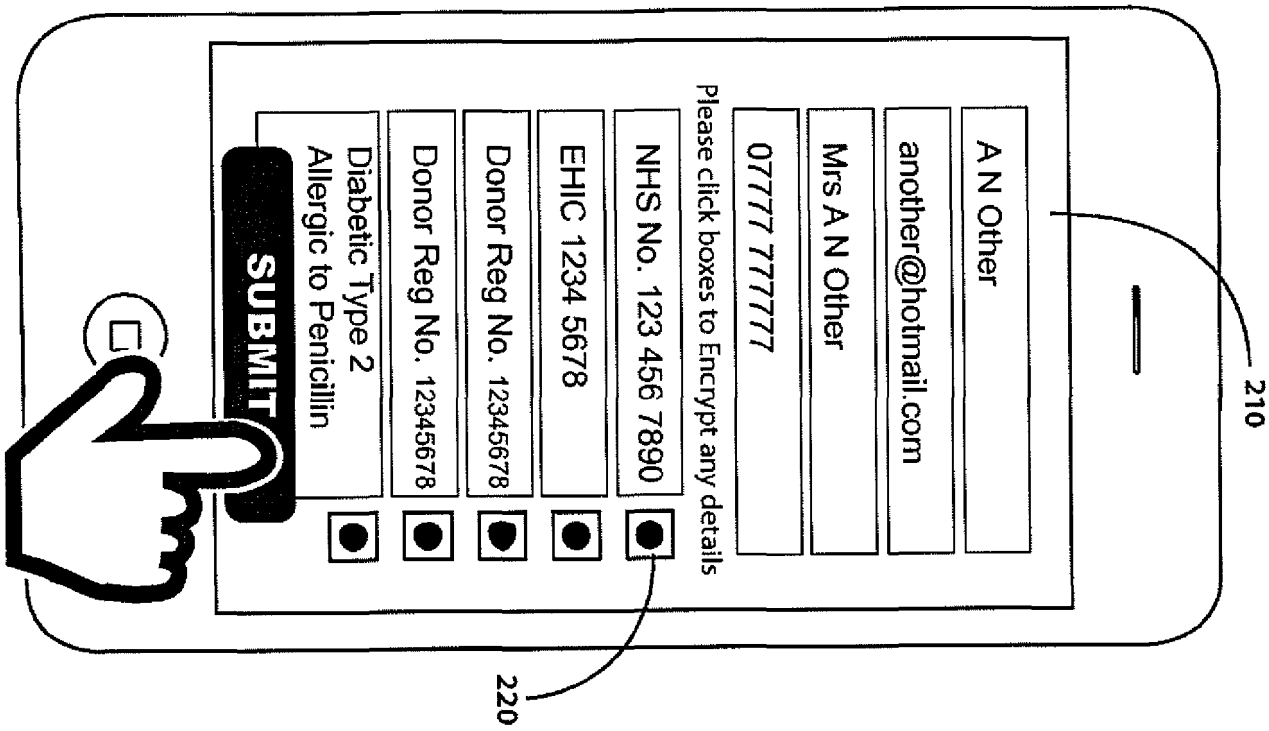
A N Other
another@hotmail.com
Mrs A N Other
07777 777777
Please click boxes to Encrypt any details
NHS No. 123 456 7890
EHIC 1234 5678
Donor Reg No. 12345678
Donor Reg No. 12345678
Diabetic Type 2
Allergic to Penicillin
SUBMIT
210
220

Fig.30

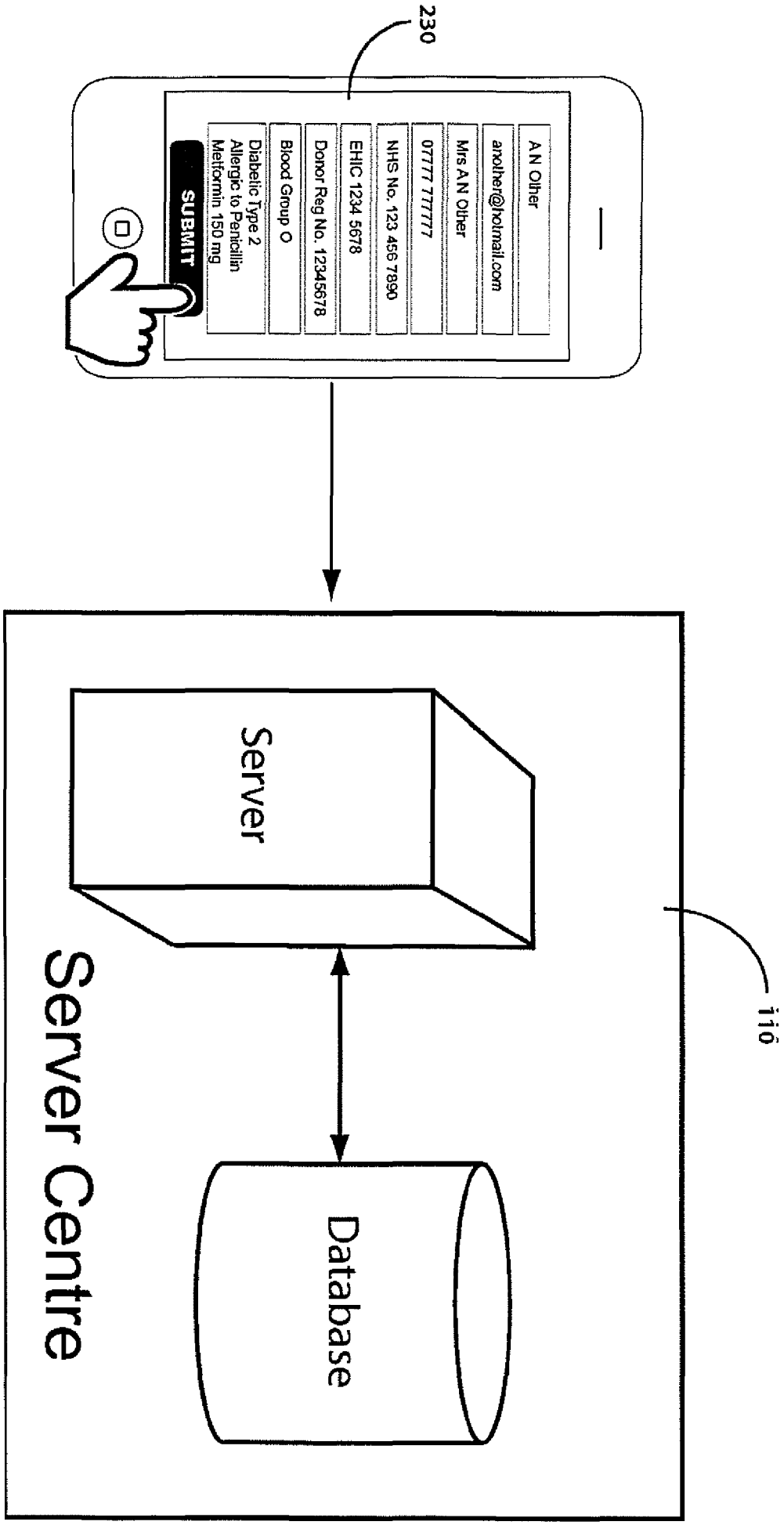
230
A N Other
another@hotmail.com
Mrs A N Other
07777 777777
NHS No. 123 456 7890
EHIC 1234 5678
Donor Reg No. 12345678
Blood Group O
Diabetic Type 2
Allergic to Penicillin
Metformin 150 mg
SUBMIT
Server
Server Centre
Database
110

Fig.40

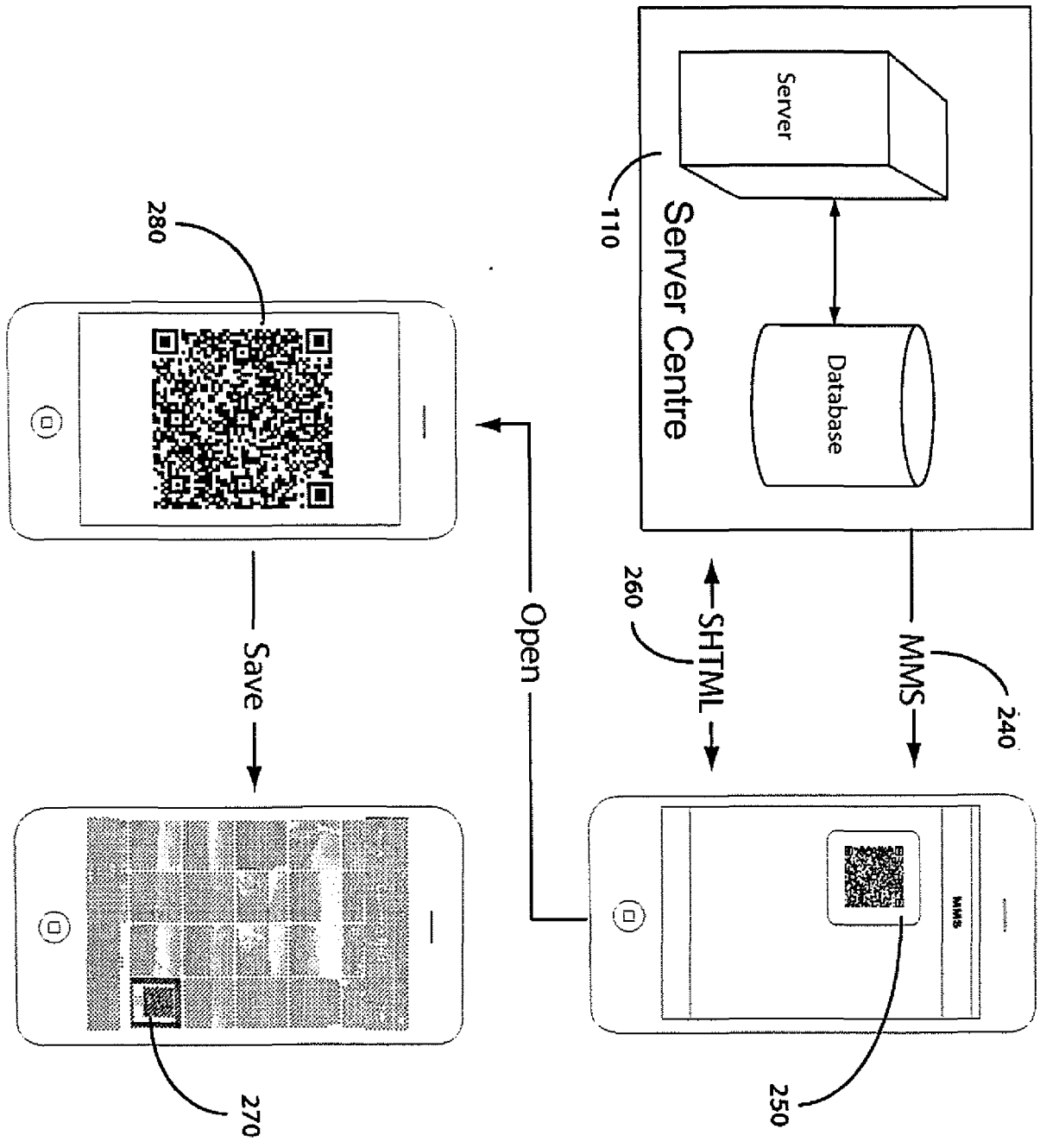
Server
Database
Server Centre
110
MMS
240
SHTML
260
Open
Save
280
270
250

Fig.50

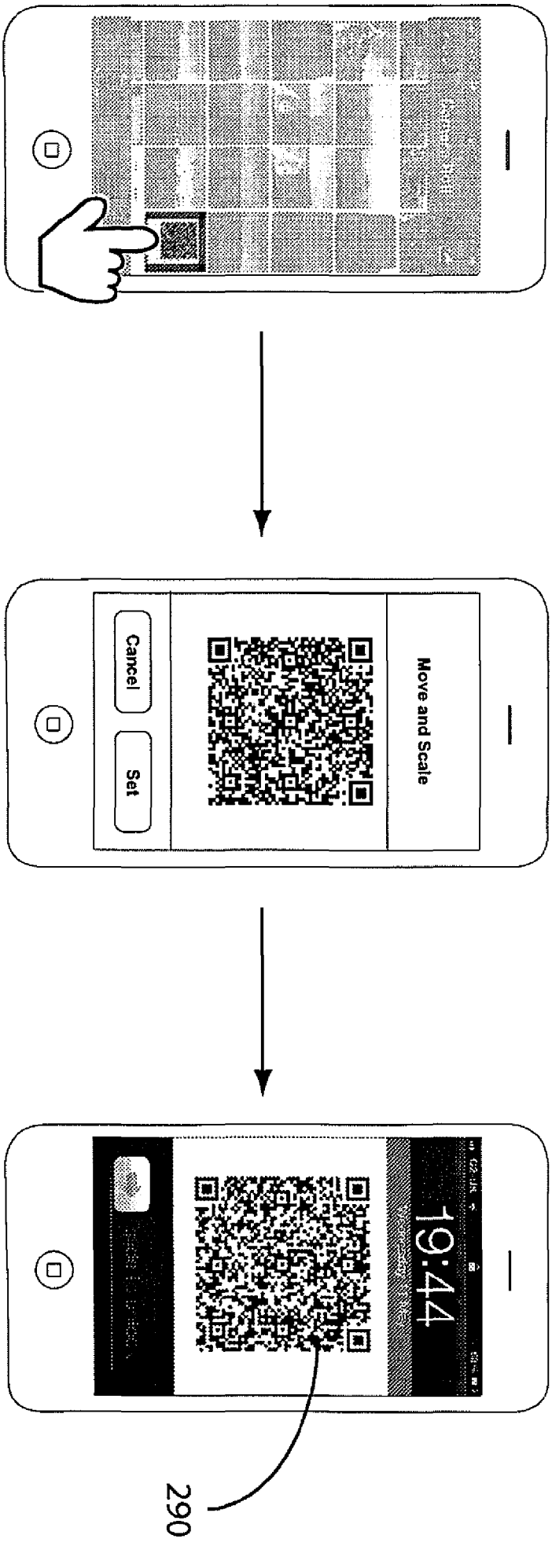

Fig.60

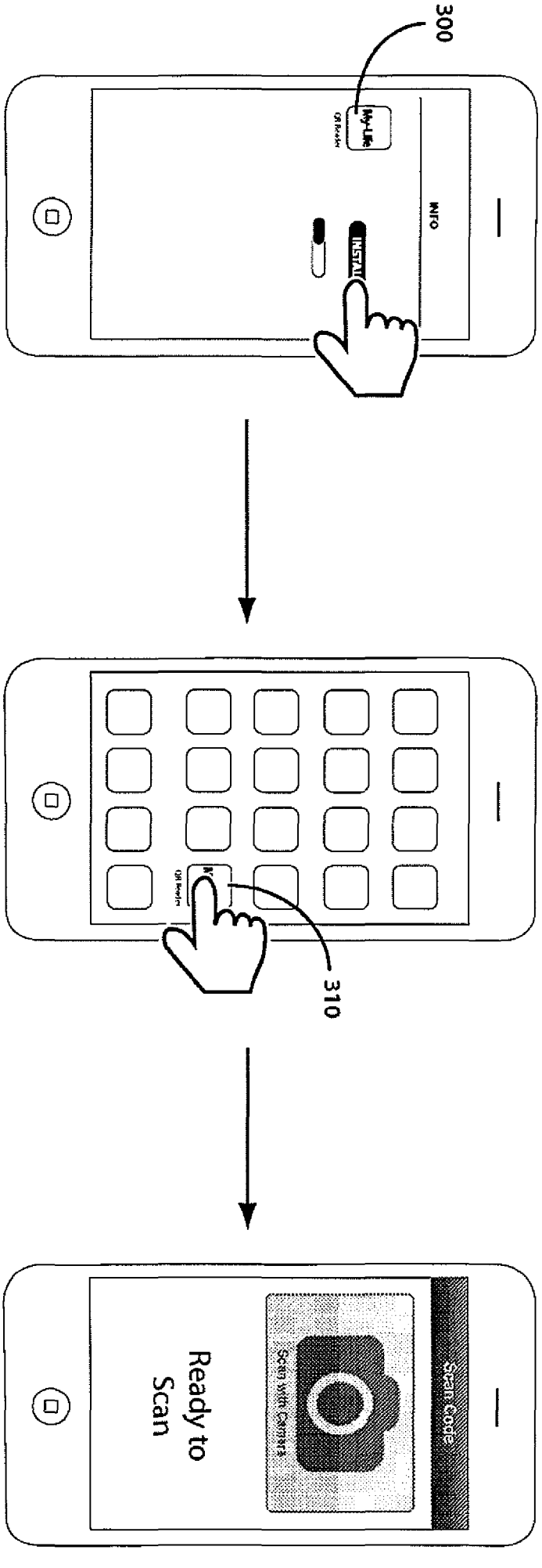

Fig.70

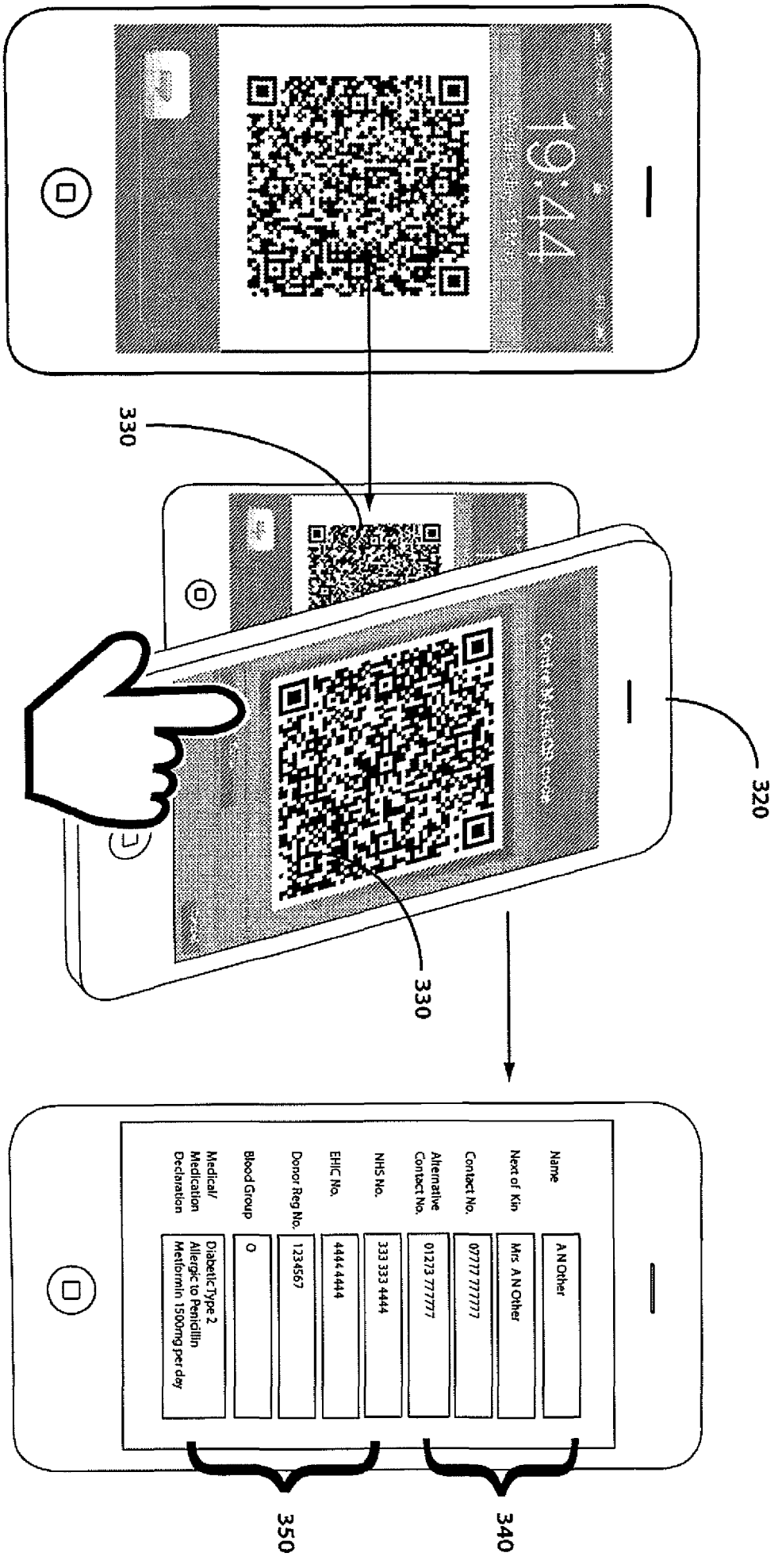
330
330
320
Name
Next of Kin
Contact No.
Alternative Contact No.
NHS No.
EHIC No.
Donor Reg No.
Blood Group
Medical/ Medication Declaration
A N Other
Mrs A N Other
07717 777777
01273 777777
333 333 4444
4444 4444
1234567
O
Diabetic Type 2
Allergic to Penicillin
Metformin 1500mg per day
340
350

Fig.8o

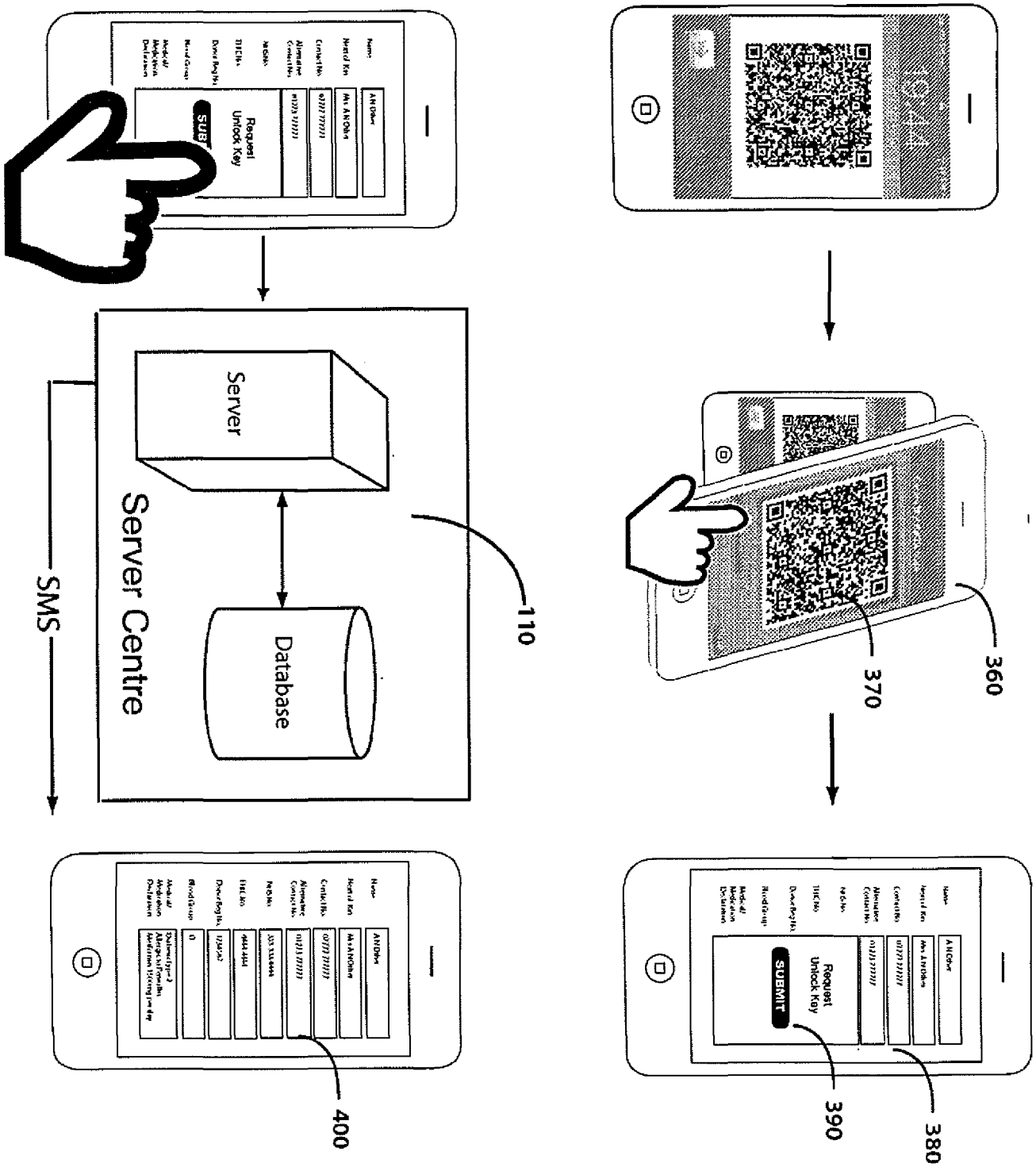
Request
Unlock Key
SUBMIT
360
370
380
390
400
110
Server
Database
Server Centre
SMS

Fig.9C

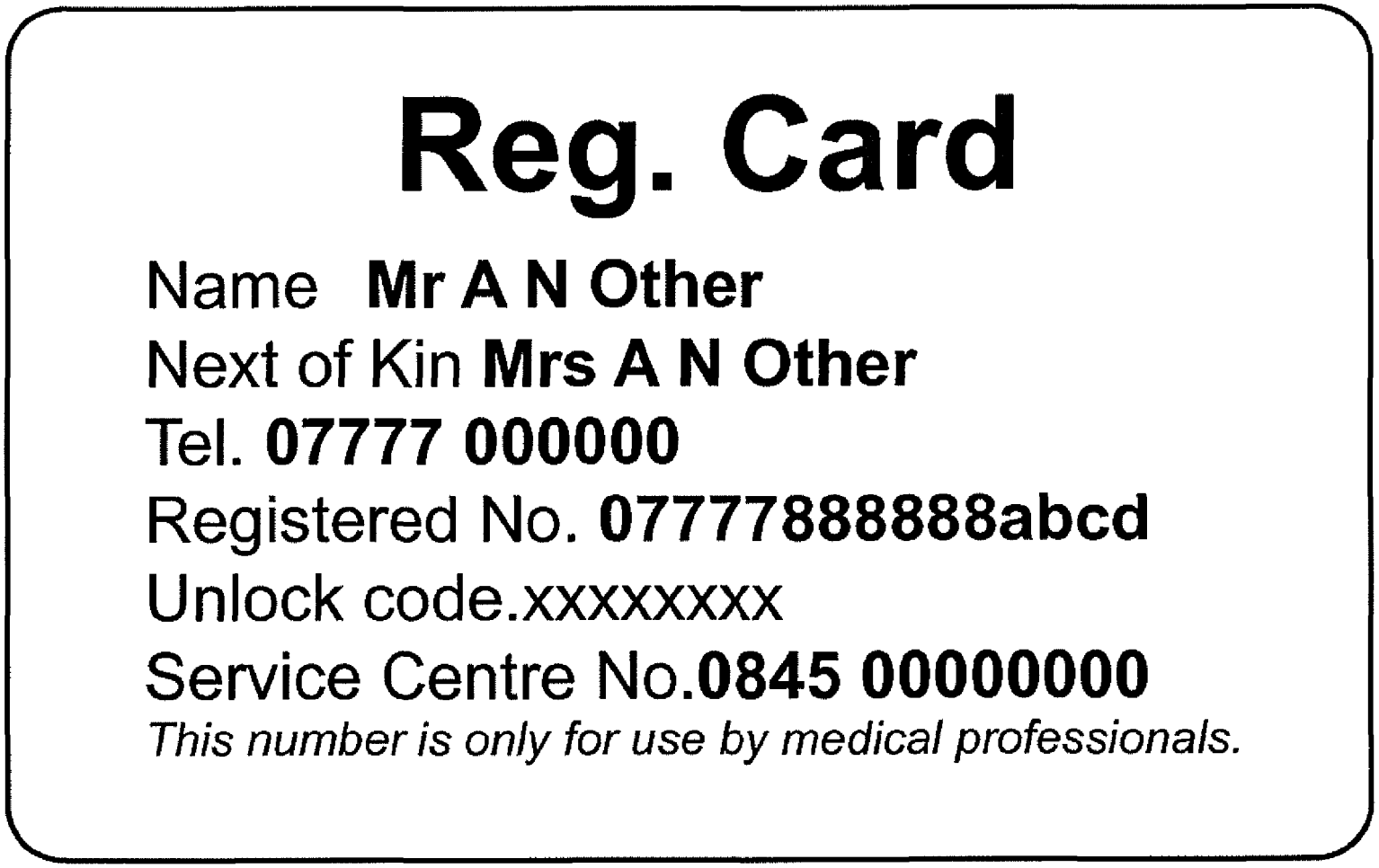
Reg. Card
Name Mr A N Other
Next of Kin Mrs A N Other
Tel. 07777 000000
Registered No. 07777888888abcd
Unlock code.xxxxxxxx
Service Centre No.0845 00000000
This number is only for use by medical professionals.

Fig.100

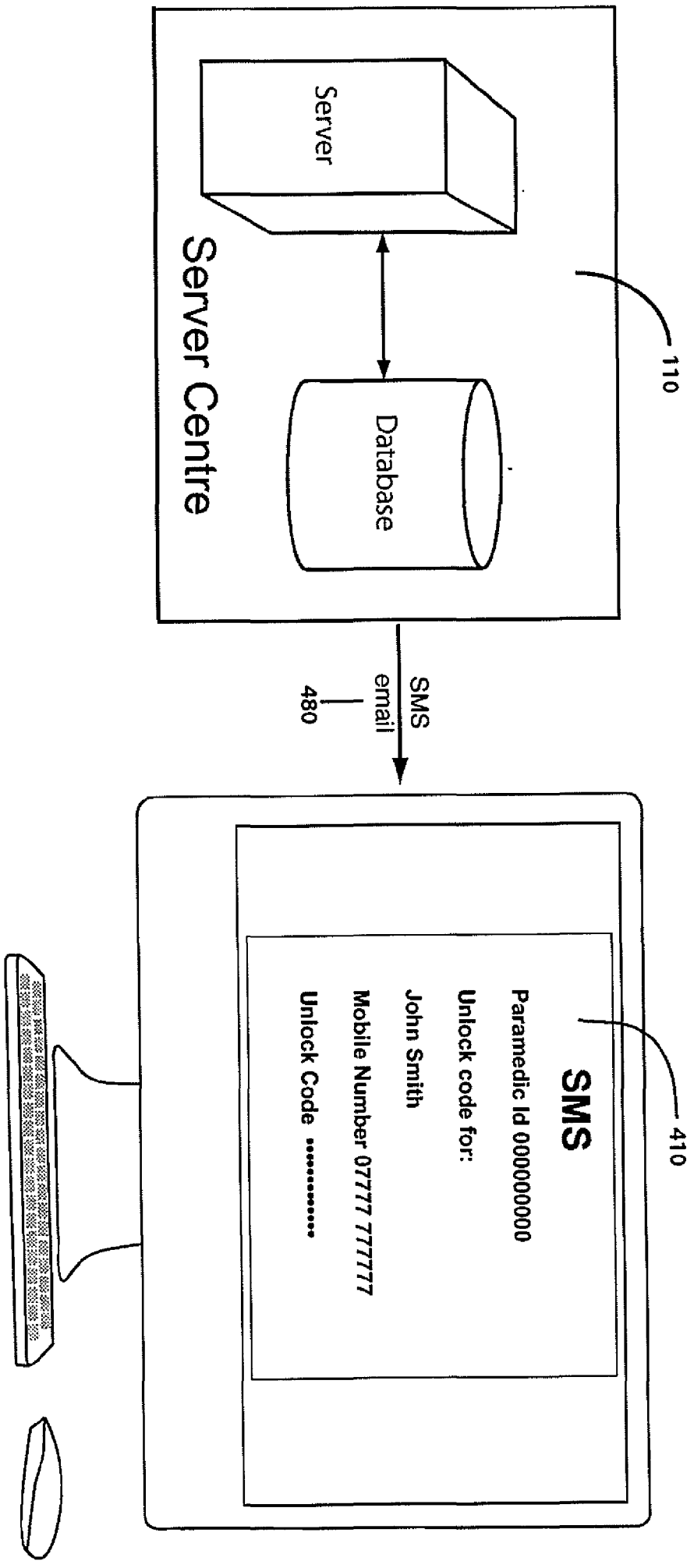
Server
Server Centre
Database
110
SMS
email
480
SMS
Paramedic Id 00000000
Unlock code for:
John Smith
Mobile Number 07777 777777
Unlock Code ••••••••••••
410

Fig.110

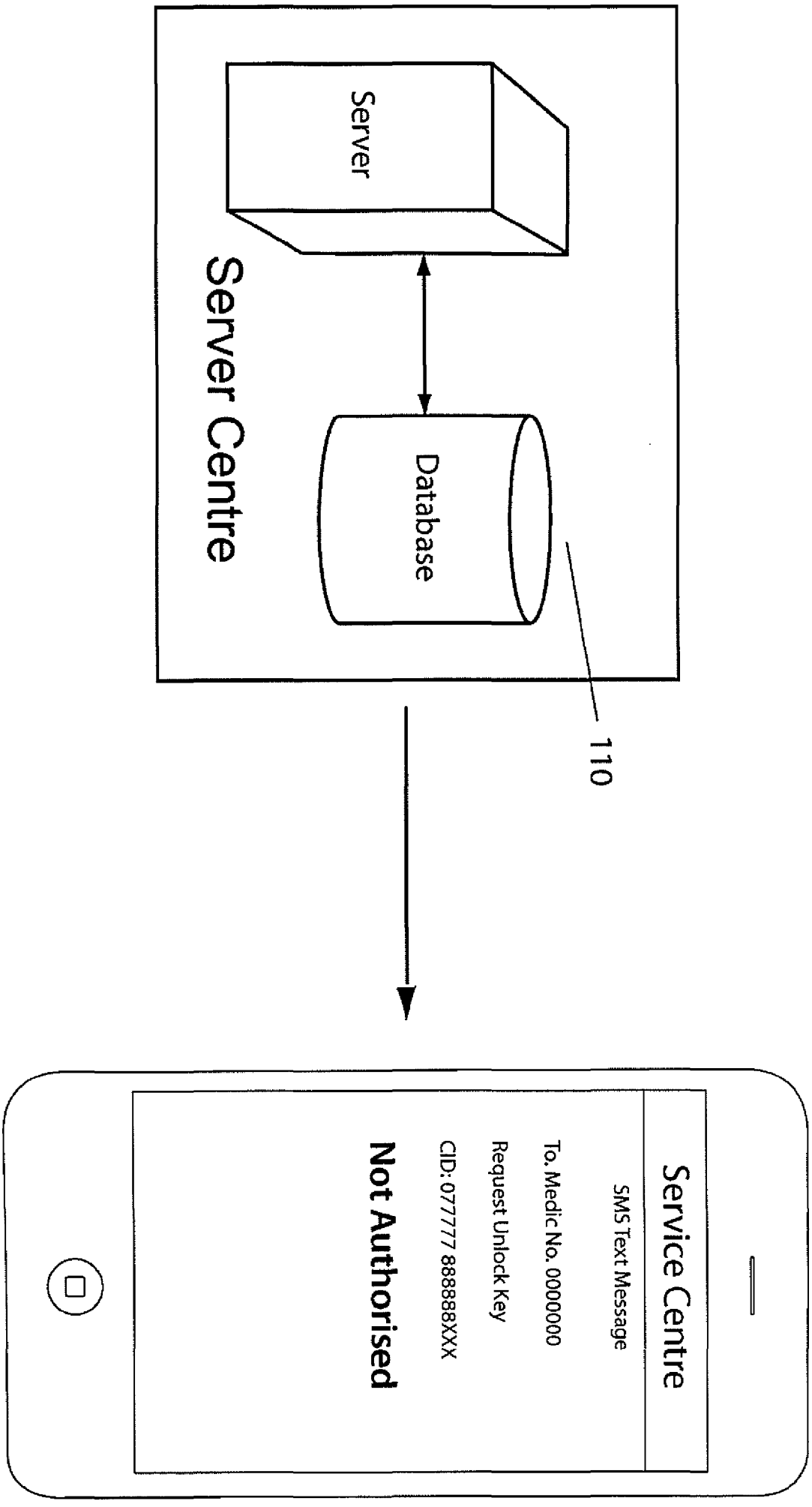
Server
Server Centre
Database
110
Service Centre
SMS Text Message
To. Medic No. 0000000
Request Unlock Key
CID: 077777 888888XXX
Not Authorised

Fig.150

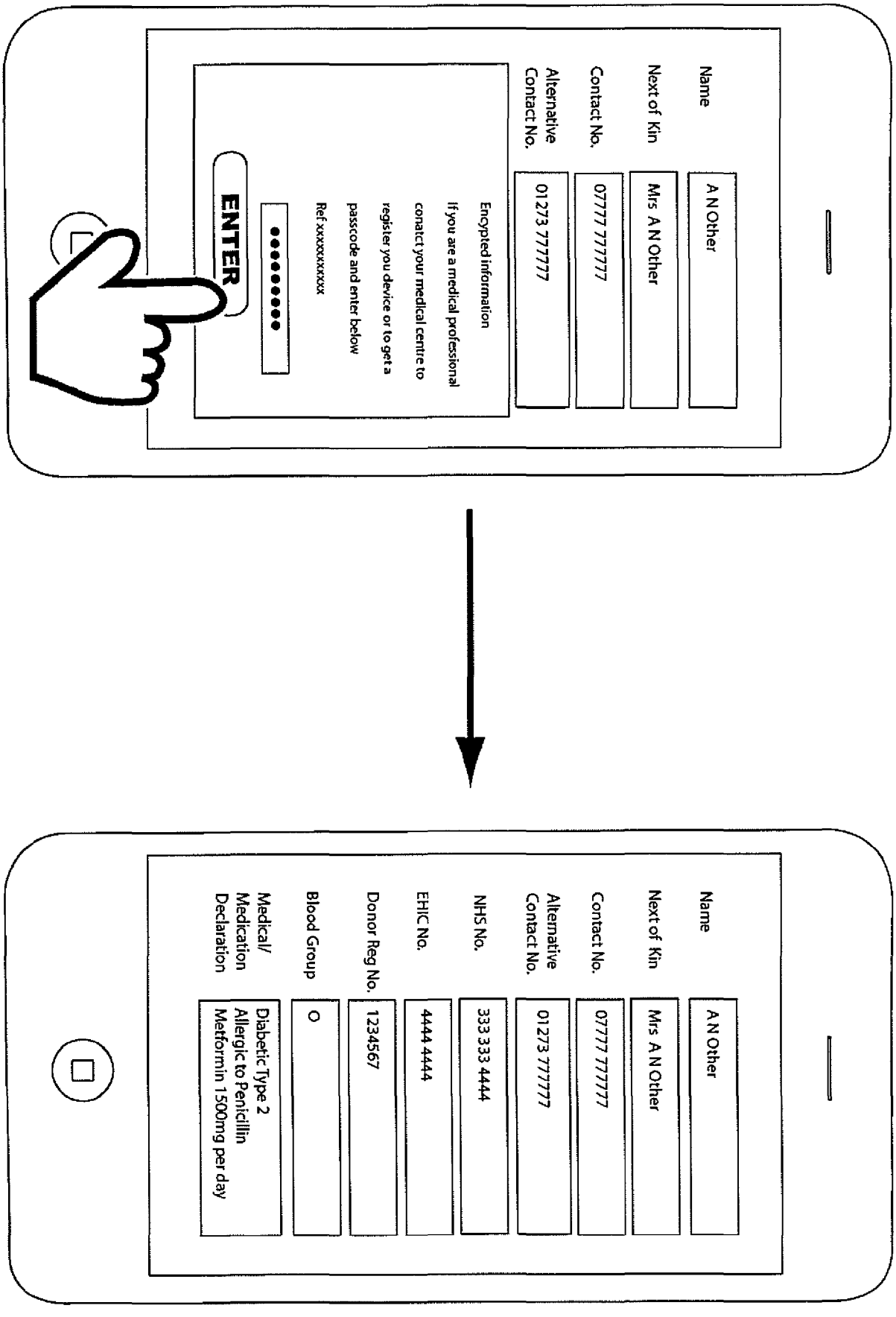
Name
A N Other
Next of Kin
Mrs A N Other
Contact No.
07777 777777
Alternative Contact No.
01273 777777
Encypted information
If you are a medical professional
conatct your medical centre to
register you device or to get a
passcode and enter below
Ref xxxxxxxxxxx
ENTER
Name
A N Other
Next of Kin
Mrs A N Other
Contact No.
07777 777777
Alternative Contact No.
01273 777777
NHS No.
333 333 4444
EHIC No.
4444 4444
Donor Reg No.
1234567
Blood Group
O
Medical/ Medication Declaration
Diabetic Type 2
Allergic to Penicillin
Metformin 1500mg per day

Fig.12O

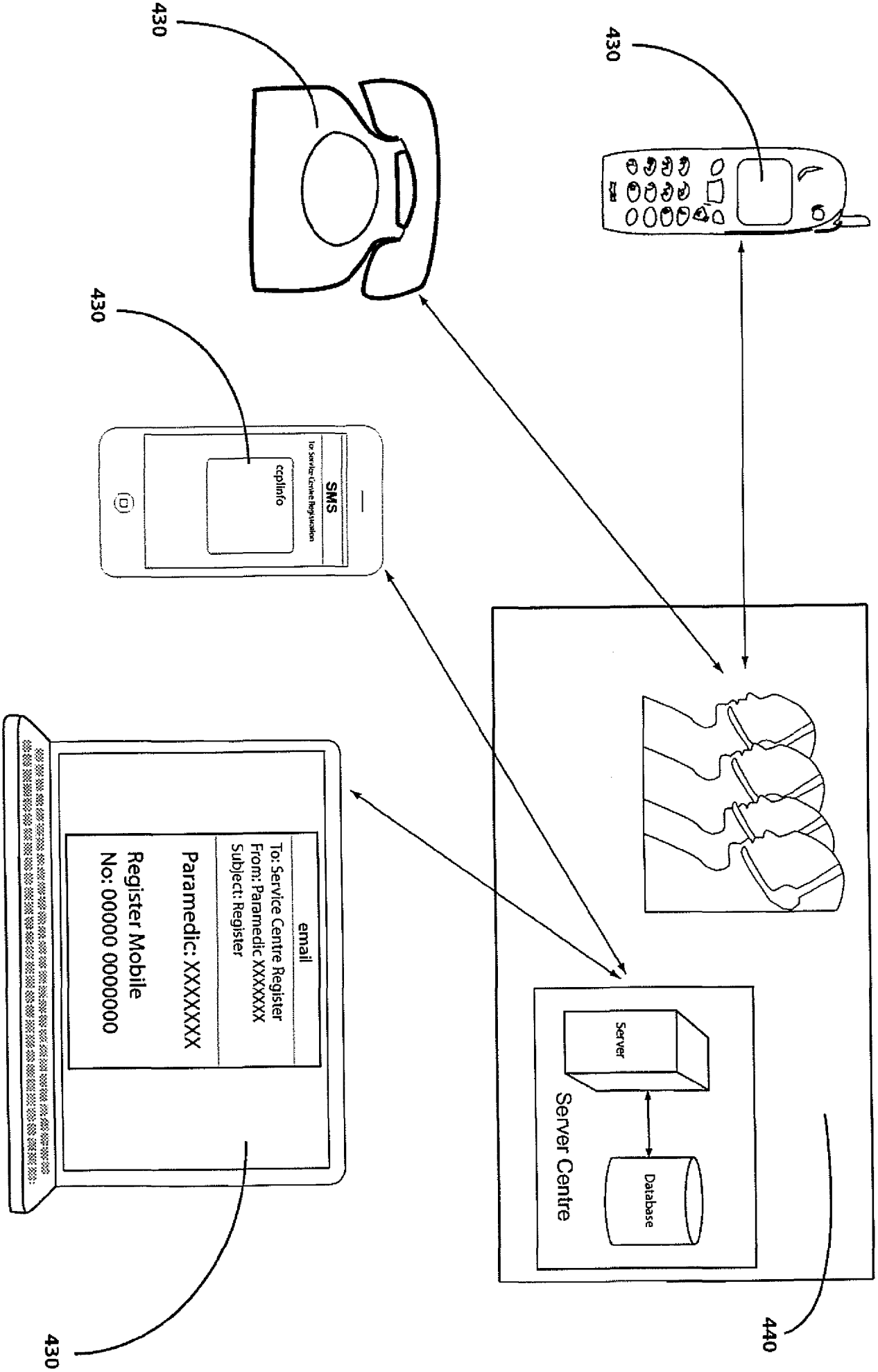
430
430
430
SMS
ccplinfo
email
To: Service Centre Register
From: Paramedic XXXXXXX
Subject: Register
Paramedic: XXXXXXX
Register Mobile
No: 00000 0000000
Server
Server Centre
Database
440
430

Fig.130

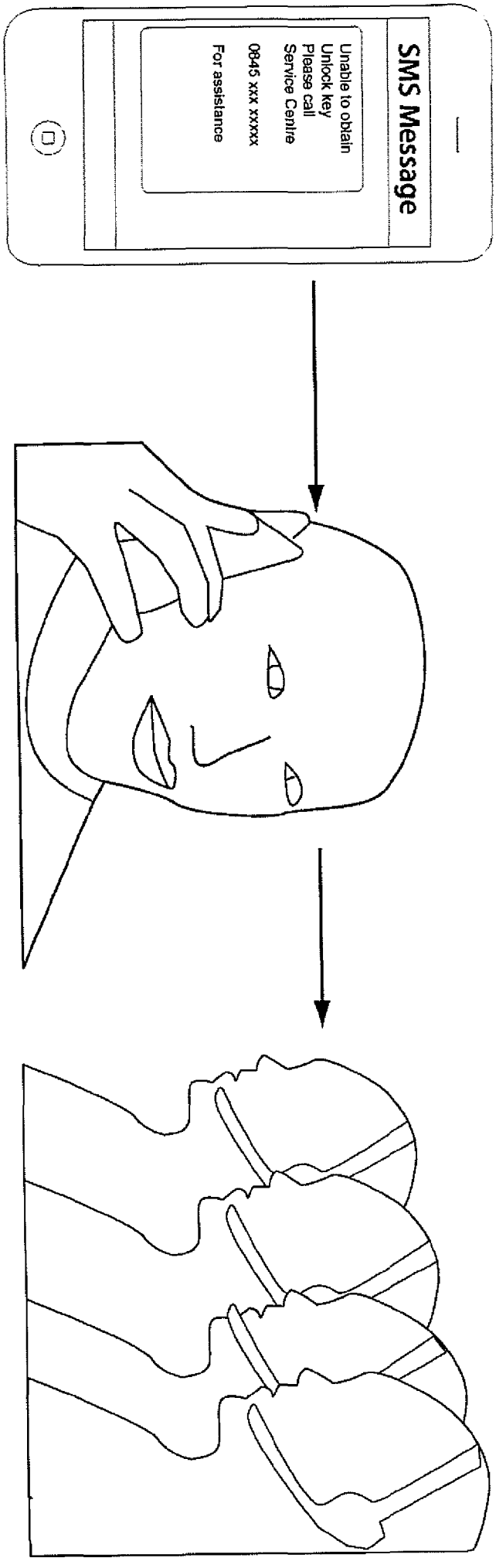
SMS Message
Unable to obtain
Unlock key
Please call
Service Centre
0845 xxx xxxxx
For assistance

Fig.160

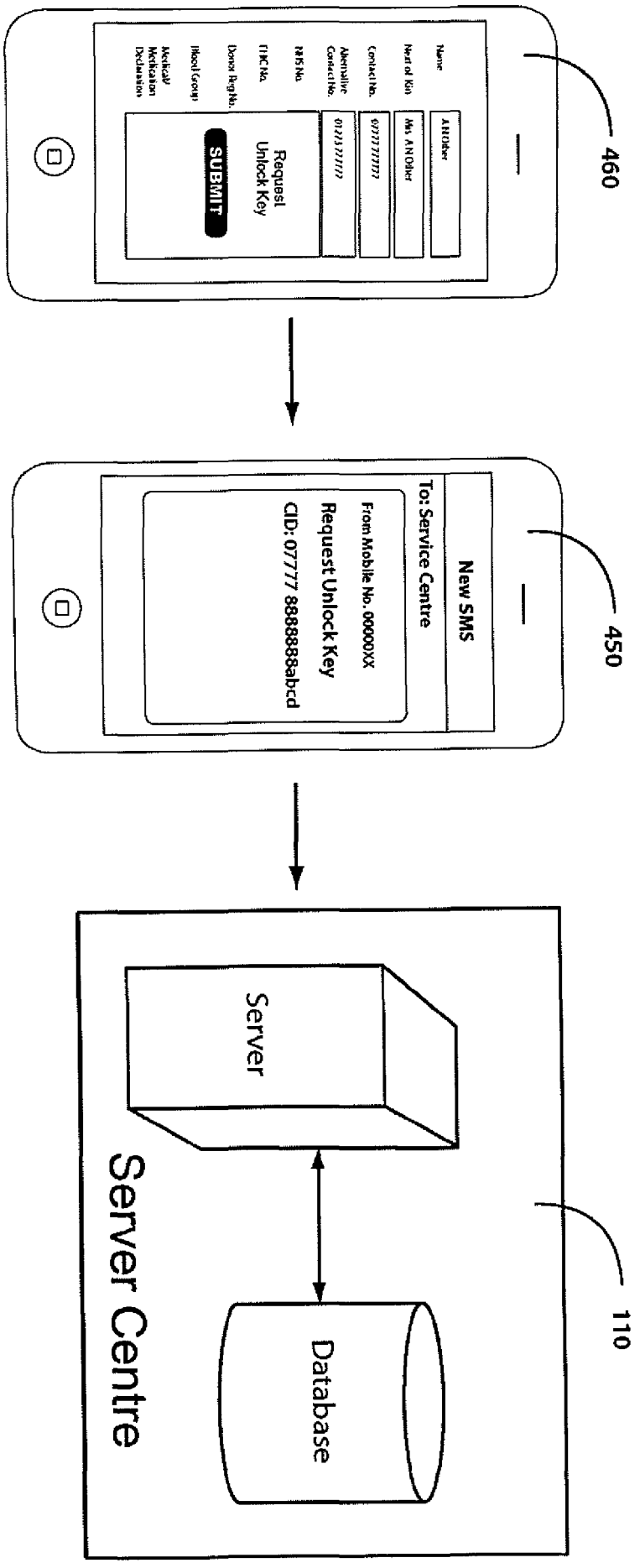
460
Name
Next of Kin
Contact No.
Alternative Contact No.
NRIC No.
Donor Reg No.
Blood Group
Medical Notification Declaration
Request Unlock Key
SUBMIT
450
New SMS
To: Service Centre
From Mobile No. 00000XX
Request Unlock Key
CID: 07777 8888888abcd
110
Server
Server Centre
Database

Fig.140

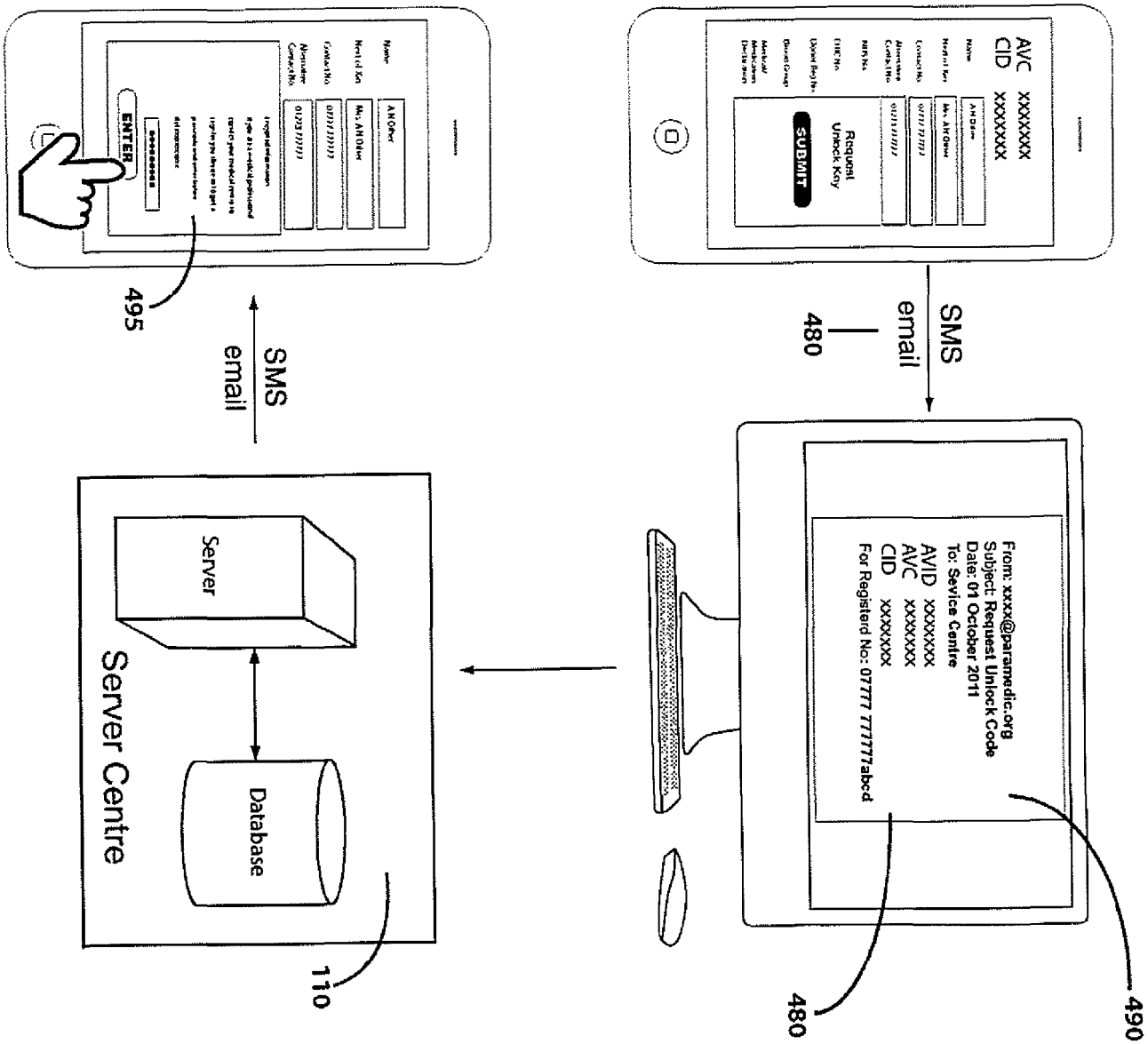
AVC XXXXXXX
CID XXXXXXX
Request Unlock Key
SUBMIT
SMS
email
480
From: xxxx@paramedic.org
Subject: Request Unlock Code
Date: 01 October 2011
To: Sevice Centre
AVID XXXXXXX
AVC XXXXXXX
CID XXXXXXX
For Registerd No: 07777 777777abcd
490
480
SMS
email
495
Server
Database
Server Centre
110

Fig.170

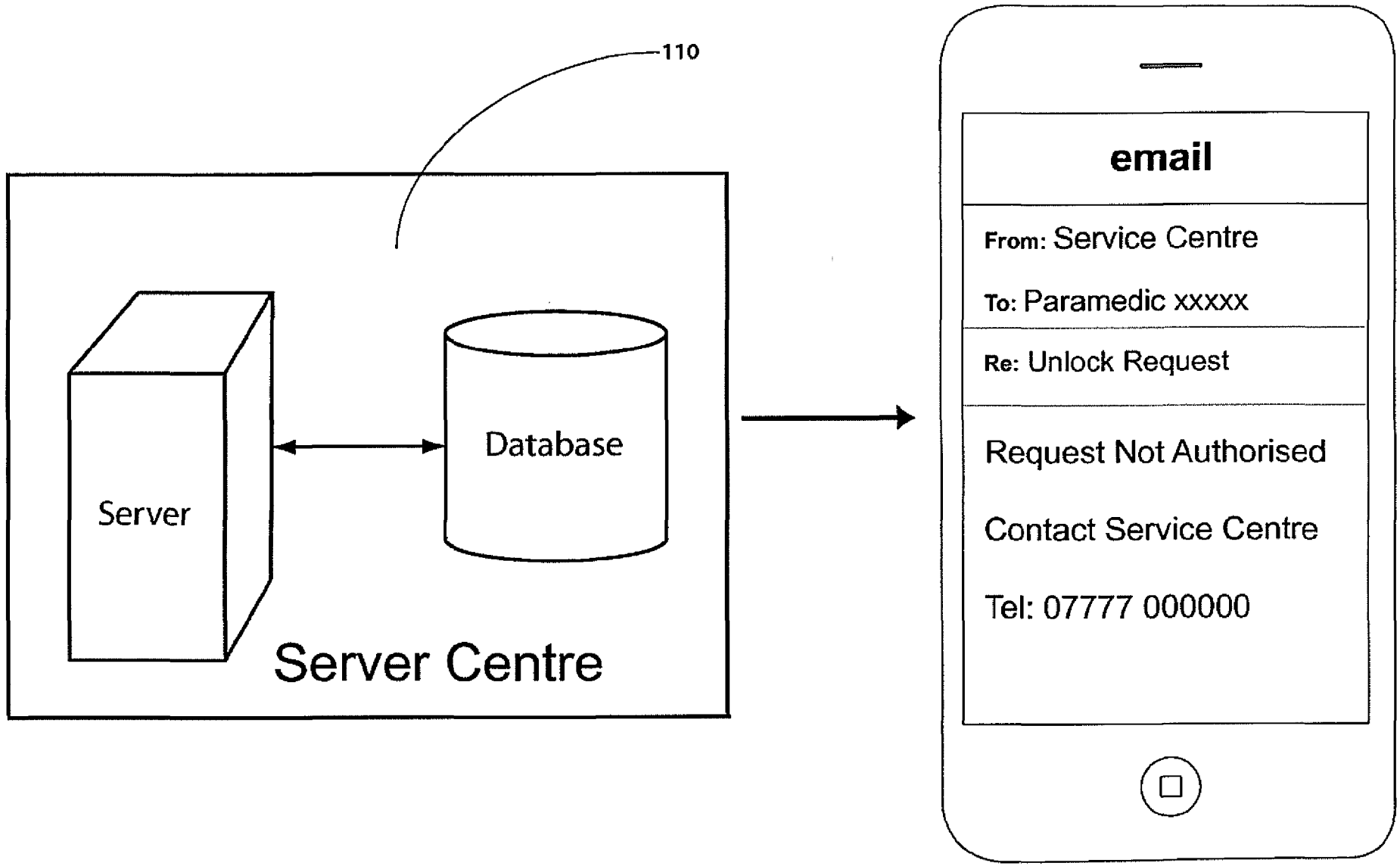
110
Server
Database
Server Centre
email
From: Service Centre
To: Paramedic xxxxx
Re: Unlock Request
Request Not Authorised
Contact Service Centre
Tel: 07777 000000

Fig.180

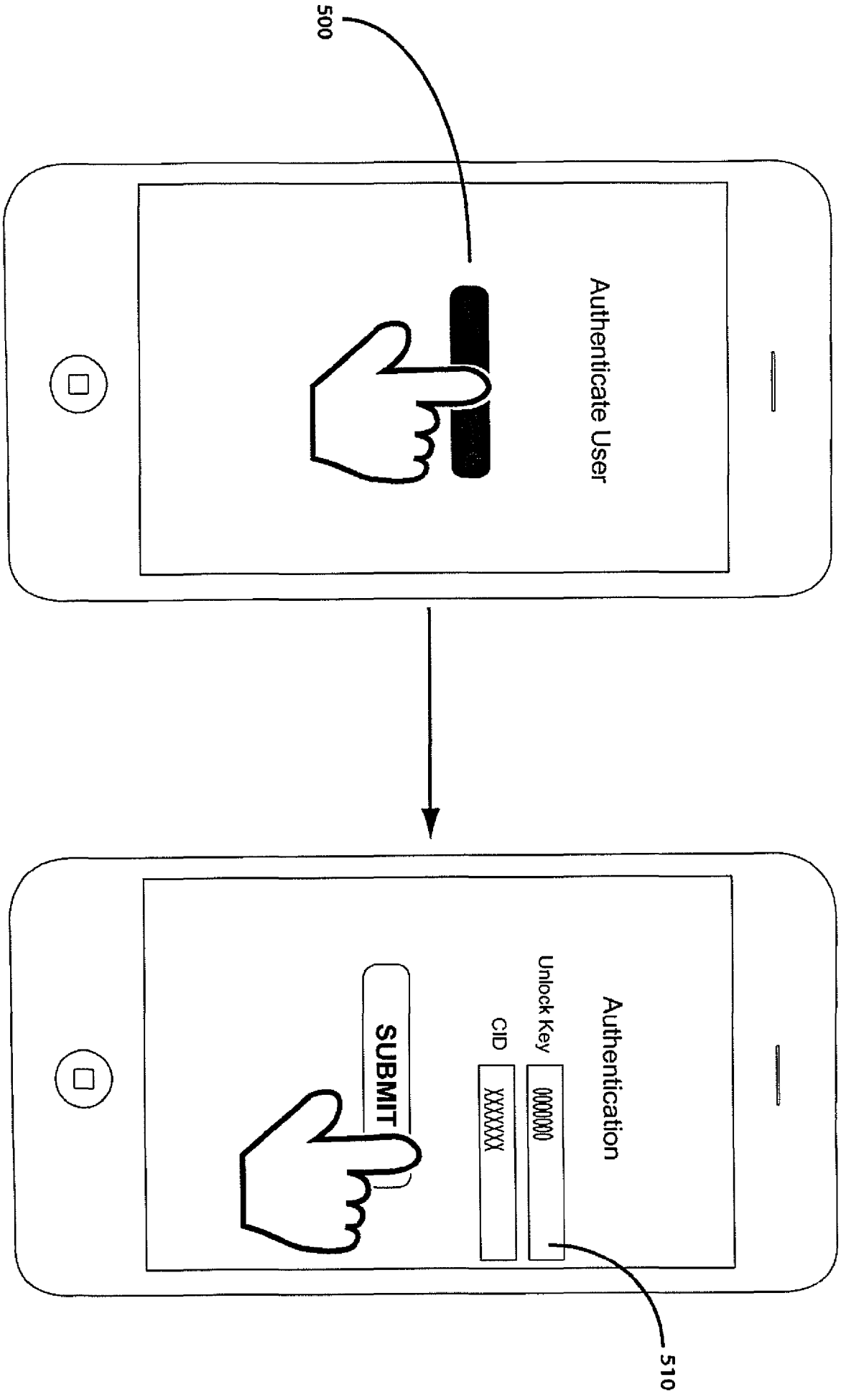
500
Authenticate User
Authentication
Unlock Key
000000
CID
XXXXXX
SUBMIT
510

Fig.190

HOLDING AND SELECTIVELY RETRIEVING INFORMATION FROM A MOBILE DEVICE DISPLAY SCREEN USING A DATA MATRIX CODE

BACKGROUND

There are times when it could be useful for a person to have about their person data which they only wish to display or communicate to other people under certain circumstances, or only to certain people. For example a person who has been in an accident and is perhaps unconscious may wish for a passer-by to be able to Unlock Key information such as their name and next of kin's contact number, but may not wish that stranger to know of certain medical conditions. However they might want paramedics to be able to view such medical data. Since the one thing many people now carry with them at all times is their mobile phone, which may be locked, it would be useful if this data could be available in encrypted form on their mobile phone, or comparable device, in this case on the front screen so that it could be viewed even if the phone is locked.

In another example, a person may wish to share contact or other personal details with someone they have met, but they may not be carrying a business card. It would be useful if they could carry something on their mobile phone from which data could be quickly transferred to the other person's phone, in such a way that they can share all or just some of their personal data.

The current invention makes such controlled sharing of information possible.

It is already possible to encode information and generate a two-dimensional DMC, for example a QR code image. Existing technology such as that for QR codes can be readily adapted (as described in this document) to place that image on a mobile phone or similar device and to place it on the front screen if required, so that it can be viewed even if the mobile device is locked.

A separate device with a built in camera, combined with a DMC decoding App can be used to read the embedded data. This is useful when the owner of the data is willing for anybody to be able to read the information.

It is not currently possible to encrypt data into a single image and allow for it to be accessed in such a way that different people can access different elements of the data.

SUMMARY OF THE INVENTION

The current invention makes it possible , inter alia, to encrypt data into a single image and allow for it to be accessed in such a way that different people can access different elements of the data.

Embodiments of the invention aim to provide a way of extracting data from a DMC image displayed on a mobile device with a data screen, such as a mobile phone or smart-phone, whereby some of the information (Secure Data) embedded in the DMC is only available to intended recipients.

The viewing of data is controlled by the use of an Unlock Key. Software running on the Reader Device viewing the DMC displays information from the DMC and if some fields are encrypted, prompts the User to provide the Unlock Key. After the correct Unlock Key has been submitted by the User then the software displays the encrypted fields.

The first embodiment of the invention aims to provide to an emergency worker, such as a paramedic or an ambulance driver equipped with a Reader Device such as a standard smart-phone, the possibility of extracting personal and medical information about a person, from that person's mobile phone.

Such information would be useful in establishing the medical history of the person while at the same time it will be possible to protect sensitive information from being accessed by non-authorised persons.

However some useful but non-sensitive data embedded in the DMC, such as the person's name and next of kin contact details, could be viewed even by non-authorised persons, for example by a passer-by at the scene of an accident,

BRIEF DESCRIPTION OF DRAWINGS

FIG.10 – Shows a Customer submit new and updated details via the service centre web GUI, on a mobile DED.

FIG.11 – Shows a Customer submit new and updated details via the service centre web GUI, on a PC based DED.

FIG.20 – Shows a Customer download an App to a smart-phone for the purpose of inputting Customer data.

FIG.30 – Shows a Customer use a smart-phone App to input Customer data.

FIG.40 – Shows a Customer request the service that generates a QR code image.

FIG.50 – Shows the Customer drag a copy of the QR code image from the web GUI to their mobile phone picture folder, which is to be displayed as a background image.

FIG.60 – Shows the QR code image displayed as a background image on the Customer phone.

FIG.70 – Shows the DRS App being downloaded to a paramedic smart-phone.

FIG.80 – Shows the RD, a dedicated QR code reader device used by paramedic staff.

FIG.90 – Shows a QR code being decoded by standard QR code reader owned by non-authorised members of the public.

FIG.100 – Shows a Customer identity card being sent from the service centre to a Customer. The card includes the Unlock Key needed to obtain medical details for the Customer.

FIG.110 – Shows an SMS message being sent from the service centre to a Customer, and which includes the Unlock Key needed to obtain medical details for that Customer.

FIG.120 – Shows a paramedic submit the Unlock Key to the DRS and subsequently being allowed to see medical records.

FIG.130 – Shows a paramedic organisation register their mobile phone numbers with the service centre.

FIG.140 – Shows the DRS App request the Unlock Key by sending an SMS message to the service centre.

FIG.150 – Shows the DRS App receive an SMS reply with the phrase "NOT AUTHORISED".

FIG.160 – Shows the DRS App recommend the user to make a voice call to the service centre

FIG.170 – Shows the DRS App request the Unlock Key by sending an email to the service centre.

FIG.180 – Shows the DRS App receive an email with the phrase "NOT AUTHORISED" included.

FIG.190 – Shows the DRS App displaying a hyper-link to the service centre GUI in order to authenticate a User before allowing access to Customer medical records.

DETAILED DESCRIPTION

For the first embodiment of the invention, Customer contact information and medical records are stored on a DCD at a secure site where access to the data is controlled by the service provider.

The service is initiated when a Customer registers their details with the service provider. In doing so the Customer is provided with a unique CID and is prompted to select a password.

The ability to update Customer information in the Service Centre is not limited to direct interaction with the Customer. It is also possible to transfer data from an

external organisation directly into the Customer data base. This would be appropriate for instance in the first embodiment where a medical facility contains information pertinent to Customer records.

INPUT AND UPDATE OF DATA

[0001] – online data entry

The Data is input by a Customer via a mobile or PC based DED while there is a secure internet connection to the DCD, which in the first embodiment is held at the Service Centre as shown in **FIG.10** and **FIG.11**. The web interface is accessed via a GUI **100** on the mobile DED or via a GUI on the PC based DED **160**.

The web interface security for the input and maintenance of Data is based upon an authentication of the Customer's registration details. For the first embodiment, when a Customer first registers with the service, they are requested to provide their name, address and mobile phone number. The service centre software creates a Customer CID. The CID is presented to the Customer in the web GUI and the Customer is prompted to create a password.

A separate data record is created for each Customer in the Service Centre Database **110**, each comprising multiple data fields. The Customer is advised that all future access to their medical details will require them to know their CID and password.

Accessing the web GUI any time after the initial registration, the Customer is prompted to provide their CID **120** and password **130** when using a mobile DED and their CID **170** and password **180**, when using a PC based DED. After being authenticated, the Customer is presented with the possibility of adding or updating Data **140** when using a mobile DED or updating Data **190** when using a PC based DED. In the first embodiment, Data input can include contact information and medical information.

Beside each Datum displayed on the mobile DED **150** or on a PC based DED **200** is a tick-box, or series of tick boxes is/are displayed, one for each Security Level which, if ticked, means that the Customer wishes the Datum to only be displayed to Authorised Users at the relevant Security Level. Such Data is treated as Secure Data. For the first embodiment, only one Security Level is provided for which Authorised Users will include for example paramedics.

If no tick-box is ticked for any Security Level against a Datum, that is taken to indicate that the Customer is willing for that Datum to be displayed to anybody reading the DMC and that Datum is treated as Open Data.

While tick boxes are used in the first embodiment, any binary method may be used to indicate whether a Security Level applies to a Datum or not. References to tick boxes in this document should be understood to include any binary indication method.

The Customer Data is stored in a database. For the first embodiment, it is stored as xml data.

[0002] – offline data entry for subsequent online transmission
A Customer is able to input data to a DED at a time when there is no internet connection to the DCD held at the Service Centre.

An App is downloaded and installed on a DED belonging to the Customer as shown in **FIG.20**.

The Customer is presented with existing values, when adding or updating Data using the App, as shown in **FIG.30**. The data records **210** displayed and the Security Level tick-boxes **220** are displayed and function as described in [0001]. The Data submitted by the Customer is held on the DED as an xml file or similar.

If the App is subsequently launched when the DED is online then an option is presented to upload the file to the DCD. When this option is selected the App attempts to log on to the server website. The Customer will then be prompted by the DCD to provide their CID and password.

After being authenticated the Customer has the option of synchronising the Data on the DED with the DCD data base version. Synchronisation is possible after the data file is uploaded from the DED to the DCD.

The DCD software application compares the date that the DED data file was updated with the date in the Data in its own database. The differences are presented to the Customer in a web page that is launched on the DED and the Customer is prompted to accept or reject the proposed updates.

[0003] – offline data entry for local QR generation
If the DED is also capable of acting as a DCD and a DD, then Data may be entered via an App installed on the DED as described in [0002], but the Data may be retained on the DED and the DMC will be generated there, as described in Methods [0004], [0005] and [0006].

GENERATING A QR CODE IMAGE

The DCD generates a DMC image after the Customer has finished adding or updating their Data.

How each Datum is embedded in the QR code depends on the Security Level that has been assigned to it.

[0004] – embedding all Data in DMC
Each Datum is coded in accordance with the Security Level tick-boxes, indicated previously as in [0001], [0002] or [0003]. The DMC contains all Data including any Open Data and any Secure Data.

If no tick-box for any Security Level has been ticked, then that Datum is classified as Open Data. For the first embodiment, Open Data is coded as standard QR code (ISO/IEC 18004:2006). It is possible that Open Data can be coded in any DMC format.

If the tick-box for a Security Level is ticked then that Datum is tagged as, Secure Data at that Security Level, and the Datum is encrypted in the DMC. This is

achieved by preceding each Secure Datum with escape characters corresponding to that Security Level.

The meaning of the escape characters is that an alternative action is required to simply displaying the corresponding field. The alternative action is to request the User to submit an Unlock Key which must be correct before displaying the Secure Data relating to that Security Level.

The first embodiment of the invention places the escape characters in position zero and one of a string, immediately followed a six digit binary coded decimal number that shall be interpreted as the Unlock Key, when the second escape character has an "on" value.

The first embodiment of the invention specifies the use of a single group of non-encrypted fields and a single group of encrypted fields. However, a relational database on a DCD can be configured to support multiple Security Levels by creating a separate table for Security Levels, where for each level data is stored concerning Authorised Users and a separate escape character is assigned to that level. In the main table where Data pertaining to each Customer is stored, a separate Unlock Key would be created and stored in respect of each Security Level used by each Customer. For each Datum, the Customer can tick one or more Security Levels to be Applicable to that Data. If at least one box is ticked then the DCD generates an Unlock Key for each Security Level and embeds it in the DMC.

When the Customer has finished updating their Data **230** then they can request the DMC image to be generated as shown in **FIG.40**.

[0005] – Secure Data via website link

The Secure Data that the Customer has accompanied with a tick in the tick-box for one or more Security Levels as specified in method [0001] or method [0002] are not included in the DMC image. Only the Open Data fields that do not have a corresponding tick in the tick-box for any Security Level are included in the DMC.

In addition to the Open Data that are included in the DMC a URL is also included, linked to the location of the DCD. The URL is accompanied by an invitation to click on the link in order to access Secure Data for the Customer.

When the Customer has finished updating their Data **230** then they can request the DMC image to be generated as shown in **FIG.40**.

[0006] – Secure Data to be communicated by Service Centre

Any Secure Datum that the Customer has accompanied with a tick in the tick-box/boxes as specified in method [0001] or method [0002], is not included in the DMC image. Only Data that do not have a corresponding tick for any Security Level are included in the DMC image.

In addition to the Open Data, Service Centre contact details are also included. The contact information is accompanied with an invitation to contact the Service Centre by telephone, SMS or other means in order to obtain Secure Data for the Customer.

When the Customer has finished updating their Data **230** then they can request the DMC image to be generated as shown in **FIG.40**.

DOWNLOADING A DMC IMAGE

After either opening the software Application on the DCD or accessing the DCD Application GUI, a Customer will see the latest DMC image corresponding to their own Data. This will be re-generated after the Customer updates their details and indicates that the update is complete or requests regeneration of the DMC.

[0007] – manual transfer

In **FIG.50**, the Customer downloads the DMC image **250** to their Display Device by copying and pasting (e.g. via an secure internet link using SHTML) **260** or otherwise manually transferring the image from the DCD directly to the appropriate folder **270** for the device in question, or alternatively the Customer requests that the DMC image is sent to their Display Device in an MMS message **240**, after which the Customer opens and transfers the enclosed DMC image to the appropriate folder **270** on the Display Device.

The image is placed in the specified location on the Display Device. For the first embodiment of the invention, the image is identified as the background image**280** to be displayed when the mobile 'phone is in standby mode, such that the image is visible even if the 'phone is locked. This enables the information to be accessed even if the Customer is unconscious or otherwise unable to unlock their 'phone. In other embodiments it may not be necessary for the image to be displayed in this location.

[0008] – automated download and placement

An App is downloaded to the Display Device. If the Customer has registered for the service, when the App is launched and the Display Device is online, the App attempts to log on to the server. The Customer is prompted for their CID and password.

Once authenticated then the App automatically downloads the latest DMC image to the Display Device and places it in the appropriate folder and location - which in the first embodiment will be the front screen visible in standby mode - as described in [0007].

READING OPEN DATA FROM THE DMC

The DMC is stored as an image **290** on the Customer's Display Device as shown in **FIG.60**. For the first embodiment it will be displayed as a background image on the front screen visible when the Display Device – in this case a mobile telephone - is locked or in standby mode .

The DMC image can be captured and decoded by a RD with DRS or GRS, in order to read any Open Data that is contained therein. To read the embedded Secure Data, a RD with DRS is required.

[0009] – normal smart-phones

Authorised Users such as paramedics and other Users such as any member of the public download DRS software **300** from the service centre website, to their Display Device **310** as shown in **FIG.70**. The DRS software is designed to allow a

User to capture a QR code image from a Customer's Display Device and display its decoded content.

The DRS displays the Open Data and, if Secure Data is also embedded, prompts the User to enter the Unlock Key relevant to any Secure Data.

The advantage of this method is that existing smart-phones can be used as Reader Devices.

[0010] – dedicated RDs
Authorised Users are supplied with specialised RDs **320** preloaded with DRS.

The specialised RD captures a DMC image **330** and displays both the Open Data **340** and the Secure Data **350**, as shown in **FIG.80**.

The advantage of this method is that the decoding of Secure Data is automatic and therefore instant, not requiring an authentication procedure.

[0011] – authorised smart-phones
Authorised Users download DRS as in method [0009]. During the download process, or at another time when the RD is connected to the Service Centre, the DRS checks whether the IMEI, serial number, SIM IMSI or other unique identifier of the RD matches any such identifier registered as an ACD on the Database. If it does match, then an adapted version of the DRS would be downloaded which would automatically display all Data embedded in a DMC to the relevant Security Level assigned to that ACD. This would enable existing smart-phones to be used as RDs and also permit rapid decoding of appropriate Secure Data.

[0012] – Generic Reader Software
If the User has an RD which carries GRS but not DRS, then they can capture the DCM and view the Open Data and the CID, but cannot view the Secure Data. For example in the first embodiment, a member of the public who has found a Customer who is unconscious after an accident could use any standard QR code reader App to read the Open Data about the Customer, including next of kin contact details, but not the Secure Data.

OBTAINING THE UNLOCK KEY
If the Customer's Display Device is found by a member of the public then the DMC **360** can be captured by another Reader Device **370** such as a smart-phone and using GRS software, the User can display Open Data **380** that is available to non-authorised Users (such as contact information), as shown in **FIG.90**.

If the DMC contains Secure Data then the User is prompted to provide an Unlock Key **390** in order to be allowed to view those parts of the Secure Data **400** relating to that Customer at the Security Level relevant to that Authorised User. The Unlock Key can be obtained by the following methods, which could be used singly or in combination.

[0013] – send physical object to carry
The Service Centre sends the Unlock Key or Keys to the Customer in the form of

an object to carry about the Customer's person, for example on a neck tag, a small card to fit in their wallet as shown in **FIG.100**, or the inside of a bracelet. The Authorised Users are instructed to look for such an object and read off the Unlock Key.

[0014] – communicate to Customer

In **FIG.110** the Service Centre communicates the Unlock Key(s) to the Customer by means of email **420**, SMS **410**, post, telephone or other means of communication. The Customer is advised to keep securely or memorise and destroy the Unlock Key(s) and the means of communication such that it is not available to unauthorised persons. They are advised to carry it discretely on their person in a manner similar to [0013], or to communicate it to the Designated User. The Authorised Users are instructed to look for such an object and read off the Unlock Key, or to ask the Customer for the relevant Unlock Key if the Customer is able to communicate it.

[0015] – communicate to Designated User

The Customer can identify someone as a Designated User, for example Next of Kin and provide contact details for them. The Service Centre communicates the Unlock Key(s) to the Designated User by means of email, post, telephone, SMS or other means of communication. Contact information for the Designated User is included in Open Data. The Authorised User is instructed to contact the Designated User, typically by telephone, to obtain the relevant Unlock Key.

[0016] – Authorised Communication Device

A User can request that a mobile device become a registered ACD by sending a message **430** using SMS, email, web access or other appropriate means of communication, to the Service Centre **440** as shown in **FIG.130**. The mobile number of the nominated mobile device is then stored in a data base at the Service Centre and the mobile device is registered as an ACD.

When requesting an Unlock Key, the User sends a message **450** by SMS, as shown in **FIG.140**, or other means from a registered ACD **460** to the Service Centre **110**. The message includes the CID of the Customer, and is a request for the Unlock Key for that Customer at the Security Level relevant to that Authorised User. The Service Centre **110** checks the identity of the communication device from which the message has been sent and compares it with the list of devices registered as ACDs. The form of identity used is most likely to be the telephone number if the device is a mobile phone or being part of an authorised closed network if the device is a radio transmitter. If the device identity does not match that of an ACD, an SMS message is returned saying NOT AUTHORISED and proposing that the user makes a voice call to the service centre, as shown in **FIG.150** and **FIG.160**. If the identity of the sending device does match that of an ACD, then the relevant Unlock Key is returned by SMS or the same other method.

[0017] - Authorised User ID

Each Authorised User is registered at the Service Centre and is allocated a unique AUID and an Authorised User Code. The AU may either supply or may change their AUC so that it is known only to them. To obtain the Unlock Key, the

Authorised User communicates **480** with the Service Centre by email, SMS, telephone or other means, as shown in **FIG.170**. The Authorised Users identify themselves with their AUID, and supply both their AUC and the CID **490**. If the AUC matches with the AUID, then the relevant Unlock Key for that Customer at the Security Level relevant to that AU is communicated to them **495** by email, SMS, telephone or other means. If the AUID is not recognised or is not matched by the AUC, then the User is advised that he/she is not authorised and it is proposed that they make a voice call to the service centre, as shown in **FIG.180**.

DECODING THE SECURE DATA IN THE DMC IMAGE

If the DMC is read from an RD with GRS, it can indicate the presence of Secure Data but cannot reveal it. An Authorised User in possession of an Unlock Key can use it to view the Secure Data at the Security Level to which that Unlock Key relates by any of the following methods.

[0018] – All Data embedded, compare unlock keys

The DMC displayed on the Customer's Display Device contains all of the Data, both open and secure, pertaining to the Customer. The DMC also contains the Unlock Key(s) as encrypted field(s).

If the User has DRS on their RD, the Open Data and CID will be displayed and the User will be invited to enter the Unlock Key to access Secure Data. After the correct number of characters has been entered, the DRS will read the Unlock Key from the DMC and compare it with the version provided by the User. If they are the same then the DRS will additionally display all Data embedded in the DMC which are preceded by the escape key relating to the relevant Security Level, as shown in **FIG.120**. If they are not the same, a message is displayed indicating that the code is incorrect and/or that access is not authorised.

[0019] – only Open Data embedded. Secure on Website, via link on RD

The DMC displayed on the Customer's Display Device contains only the Open Data pertaining to the Customer. The DMC also contains a link **500** to the DCD where Secure Data pertaining to the Customer can be found, as shown in **FIG.190**.

When following the link to the secure web site, the User is prompted to provide the CID and Unlock Key **510**. This can be done either on the RD, before the link is enabled, or at the website after the link has been followed.

If the Unlock Key provided by the User is valid then the User is redirected to another web page where they have access to the Customer's Secure Data, as shown in **FIG.120**.

[0020] – only Open Data embedded. Secure Data on Website, not from RD

An Authorised User with access to the internet can access the website directly from any device. If they enter a CID and a correct Unlock Key, they will be taken to a webpage displaying all of the Customer's Data up to the relevant Security Level. No data will be displayed on the website without provision of either a correct Customer password or a correct Unlock Key.

GLOSSARY OF TERMS

App	A piece of software designed to perform a specific task that can be installed on to a smart-phone or other DED, DCD, DD or DD
Authorised User	A person authorised to view the data embedded in the DMC, identified as having a specified Security Level
AUID	Authorised User Identity; A unique identifier for an Authorised User
AUC	Authorised User Code; A secure password validating the identity of that Authorised User
ACD	Authorised Communication Device; A uniquely identifiable communications device or RD such as a mobile phone which has been registered with the Service Centre as being under the control of an identified Authorised User
Customer	A person who carries on their Display Device a DMC holding encrypted Data
CID	Customer Identity, a unique identifier for that Customer
Data	Any data entered onto the database by a Customer or encrypted in the DMC. For the first embodiment of the invention, the Data will mainly be personal data including medical data pertaining to the Customer
Datum	A particular item of Data represented by the value captured in one field for one record in the Database
DCD	Data Capture Device; any device capable of being configured to enable it to receive data from a Data Entry Device, to store and re-transmit that data, to generate a DMC embedding that data. For the first embodiment the DCD will be a secure server with internet connection

DED	Data Entry Device; any device capable of being configured to enable the input of data, it's transmission to a Data Capture Device, and/or subsequent receipt of that data from the Data Capture device in the same form, for viewing, editing and retransmission. For the first embodiment the DED will be a smart-phone or a PC connected to the internet
DMC	Data Matrix Code; a two dimensional code or barcode such as a QR code capable of embodying data in the form of an array of areas of light and dark which can be interpreted by a suitable RD to reveal the embodied data. In the first embodiment of the invention, the DMC used will be a QR code.
Database	A means of storing data in digital form, including xml files
DD	Display Device; any digital device capable of displaying a DMC, including a computer and typically a mobile phone. For the first embodiment the DD is a mobile phone, including but not limited to a smart-phone
DRS	Dedicated Reader Software which runs on a Reader Device, enabling the data embedded in a DMC to be displayed in a specialised format
GRS	Generic Reader Software; Any software able to display the embedded data which is not Dedicated Reader Software, Includes standard QR-Code-reader Apps
GUI	Graphical User Interface
HTML	Hyper Text Protocol
MMS	Multi Media Messaging service
Open Data	Data for which no Security Level has been selected positively

QR code	Quick Response code; a type of two-dimensional matrix barcode designed to be read by smart-phones. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL, or other data
PC	Personal Computer
RD	Reader Device: a device capable of scanning and interpreting the data embedded in a DMC, such as a smart-phone
Secure Data	Data for which one or more Security Levels has/have been selected positively
Security Level	A grouping or category of Authorised Users and a corresponding grouping of records in a database which have been identified by the Customer as being suitable to be viewed by the same category of Authorised User
Service Centre	A unit providing information to Customers and Authorised Users including Unlock Keys, drawing on Data in the DCD
Service Provider	The body or bodies managing the Database and/or the Service Centre
SHTML	Secure HTML
Smart-phone	Electronic handheld device that integrates the functionality of a mobile phone, personal digital assistant (PDA) or other information Applianceincluding the functionality of a camera
Unlock Key	code which may be applied to give access to the Secure Data
User	A person attempting to view the Data embedded in a DMC

CLAIMS

1. A method for encoding information into a data matrix code, whereby the data matrix code is displayed on the screen of a mobile communications device, and whereby some of the information can only be decoded and then viewed by authorised viewers, comprising:

(a) A server application program that allows a user of the application to logon and submit information, and convert the information into a data matrix code and download the data matrix code to a mobile communications device where it is displayed as a background image on the screen of the mobile communications device.

(b) A mobile application that when installed on a mobile phone or mobile smart phone with a camera facility, enables the mobile phone or mobile smart phone to capture an image of a data matrix code that is displayed on another mobile communications device, and decode the image into information that is then displayed on the screen of the mobile phone or mobile smart phone.

2. The method in claim 1, wherein the said information that is encoded into a data matrix code, is a person's contact details and also medical records.

3. The encoded information in claim 1, wherein the said information when displayed on the mobile phone or mobile smart phone, includes an indication that there are encrypted data fields contained in the said data matrix code.

4. The server application program of claim 1, wherein the said application program authenticates users and accepts data from users via a graphical user interface over the world wide web, and has an interface to a secure, co-located data base, wherein information submitted by users using the graphical user interface is stored.

5. The data matrix code in claim 1, wherein the said data matrix code is a Quick Response Code.

6. The data matrix code in claim 1, wherein part of the information contained in the data matrix code is withheld from unauthorised persons, using an encryption process.

7. The encryption process in claim 6, wherein the encoding of the said data matrix code includes the placing of an escape character in the first position, on the same line, and preceding the character string that is being encrypted.

8. The encryption process in claim 6, wherein the encoding of the said data matrix code includes the placing of the integer value one in the second character position, on the same line, and preceding the character string that is to be encrypted.

9. The encryption process in claim 6, wherein the encoding of said data matrix code includes the placing of an unlock key, consisting of a series characters, in the character positions from character position three, on the same line, and preceding the string that is to be encrypted.

10. The encryption process in claim 6, wherein the encoding of said data matrix code includes the placing of the string that is to be encrypted, in the character positions following the last character of the unlock key, on the same line.

11. The server application program of claim 1, wherein the application program is operable to:

In response to a request from a user to update personal contact details or medical records, determine whether said user is authorised to perform such actions.

When said user is determined to be authorised to update personal contact details or medical records, pull the said user's personal contact details and medical records from the data base and present the details on the graphical user interface.

When the said user is determined to be not authorised to update personal contact details or medical records, reject the request with a notification that the said user is either not authorised or that the said user is not registered.

12. The server application program of claim 1, wherein the application program is operable to:

In response to a request from the said user to encode personal contact details and medical records, into a data matrix code, determine whether the said user has requested that some of the information is not to be displayed to unauthorised persons when the said data matrix is decoded.

When it is determined that the said user has requested that some of the information is not to be displayed when the said matrix is decoded, when encoding the information fields in a matrix code then insert an escape character immediately before the information fields.

When it is determined that the said user has requested that all of the information is to be displayed when the said matrix code is decoded, when encoding the information fields in a matrix code then do not insert an escape character immediately before the information field.

13. The server application program of claim 1, wherein the application program is operable to:

In response to a Short Message Service message with a request for the unlock code for a given user, identified by a unique identity, determine whether the mobile phone number of the sender of the Short Message Service message is allowed to receive the said unlock code.

When it is determined that the mobile phone number of the sender of the Short Message Service message is authorised, read the unlock number for the user identity and send a Short Message Service message response to the mobile phone number of the sender, with the unlock key contained in the Short Message Service message response.

When it is determined that the mobile phone number of the sender of the Short Message Service message is not authorised, send a Short Message Service message response to the mobile phone number of the sender, with text indicating that the mobile phone number is not authorised contained in the Short Message Service message response.

14. The server application program of claim 1, wherein the application program is operable to:

In response to an email with a request for the unlock code for a given user, identified by a unique identity, determine whether the mobile phone number of the sender of email is allowed to receive the said unlock code.

When it is determined that the mobile phone number of the sender of the email is authorised, read the unlock number for the user identity and send an email response to the mobile phone number of the sender, with the unlock key contained in the email response.

When it is determined that the mobile phone number of the sender of email is not authorised, send an email response to the mobile phone number of the sender, with text indicating that the sender of the email is not authorised contained in the email response.

15. The server application program of claim 1, wherein the application program is operable to:

In response to a Short Message Service message with a request for the unlock code for a given user, identified by a unique identity, determine whether the enclosed identity of the sender of the Short Message Service message is allowed to receive the said unlock code.

When it is determined that the sender of the Short Message Service message is authorised, read the unlock number for the user identity and send a Short Message Service message response to the mobile phone number of the sender, with the unlock key contained in the Short Message Service message response.

When it is determined that the sender of the Short Message Service message is not authorised, send a Short Message Service message response to the mobile phone number of the sender, with text indicating that the user is not authorised contained in the Short Message Service message response.

16. The server application program of claim 1, wherein the application program is operable to:

In response to an email with a request for the unlock code for a given user, identified by a unique identity, determine whether the enclosed identity of the sender of the email is allowed to receive the said unlock code.

When it is determined that the sender of the email is authorised, read the unlock number for the user identity and send an email response to the mobile phone number of the sender, with the unlock key contained in the email response.

When it is determined that the sender of the email is not authorised, send an email response to the mobile phone number of the sender, with text indicating that the sender of the email is not authorised contained in the email response.

17. The mobile application of claim 1, wherein the application is operable to:

When decoding a data matrix code, examine the first character of each string and determine if the character is an escape character.

When it is determined that the first character of the string is an escape character, then the mobile device shall initiate a decryption process.

When it is determined that the first character of the string is not an escape character then the mobile device shall display the remaining characters of the string on the screen of the mobile device.

18. The decryption process of claim 17, wherein the process is operable to:

When reading the second character of the string, determine if the character is equal to the integer value one.

When it is determined that the character is equal to the integer value one then the process shall read the unlock key which is embedded in the string immediately following the second character, and prompt the user of the mobile device to key in the unlock key via the mobile device keypad.

19. The decryption process of claim 17, wherein the process is operable to:

When validating the string that has been keyed in via the keypad of the mobile device, determine if the value of the string is the same as the unlock key that is embedded in the decoded string therein of claim 14.

When it is determined that the string is the same as the unlock key that is embedded in the decoded string then the remaining characters in the decoded string are displayed on the display screen of the mobile device.

When it is determined the string is not the same as the unlock key that is embedded in the decoded string then the user is informed with an appropriate notification displayed on the display screen that the user is not authorised to view the encrypted string.

Application No:	GB1201370.2	**Examiner:**	Mr Alan Phipps
Claims searched:	1-19	**Date of search:**	24 May 2012

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
Y	1,2,4-19	US 2010/219241 A1 CORWIN et al., see whole document, notably Figure 2
Y	1,2,4-19	US 2006/144946 A1 VERITEC, see notably paragraphs 4,26 and Fig. 5
A	-	GB 2459686 A TRINITY MOBILE, see whole document
A	-	www.isavemylife.com see whole disclosure

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

G06K

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

WPI, EPODOC

International Classification:

Subclass	Subgroup	Valid From
G06K	0019/06	01/01/2006
G06K	0007/14	01/01/2006