(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 June 2011 (03.06.2011)

PCT

(10) International Publication Number
WO 2011/065910 A1

(51) International Patent Classification:
G06F 17/30 (2006.01) *G06Q 50/00* (2006.01)
G06F 21/00 (2006.01) *A61B 5/00* (2006.01)

(21) International Application Number:
PCT/SE2010/051307

(22) International Filing Date:
26 November 2010 (26.11.2010)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
0950910-0 27 November 2009 (27.11.2009) SE

(72) Inventor; and
(71) Applicant : **BERGSTEDT, Britta** [SE/SE]; Antilopvägen 2, S-181 43 Lidingö (SE).

(74) Agent: **GROTH & CO. KB**; Box 6107, S-102 32 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: SYSTEM COMPRISING DATABASE AND SAFETY DEVICE

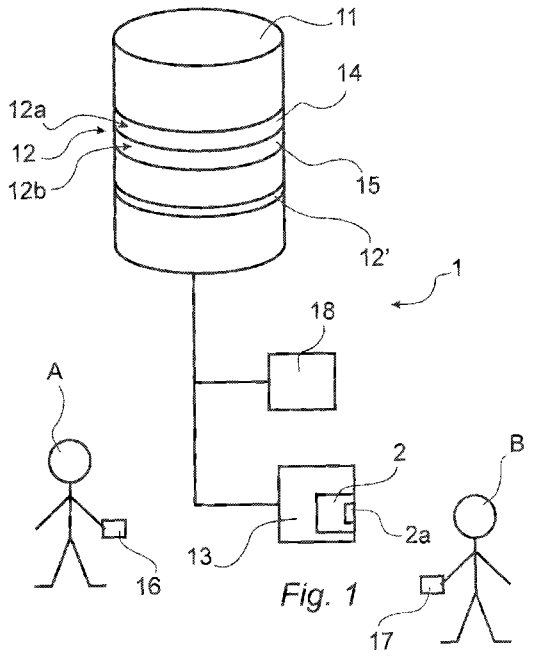

Fig. 1

(57) Abstract: The present invention relates to a system (1) comprising a database (11), where in the database, there is stored personal information (12) regarding at least one individual (A), which information (12) comprises information regarding the individual's state of health. The system (1) also comprises a safety device (13) adapted to protect at least parts of the information (12) against unauthorized access. The present invention teaches particularly that the database (11) is divided into a first storage space (14) and a second storage space (15), where the safety device (13) is adapted to grant an authorized user (B) access to the first storage space (14) according to a first safety level and to the second storage space (15) according to a second safety level. In the first storage space (14), there is stored general information (12a) about the individual's (A) state of health, and in the second storage space (15), there is stored specific information (12b) about the individual's (A) state of health. The safety device (13) is adapted to demand a first authorization key (16) belonging to the individual (A) in combination with a second authorization key (17) belonging to the authorized user (B) in order for access to the first storage space (14) to be granted to the authorized user (B).

WO 2011/065910 A1

Published:

— *with international search report (Art. 21(3))*

SYSTEM COMPRISING DATABASE AND SAFETY DEVICE

TECHNICAL FIELD

The present invention relates to a system comprising a database, where in the database, there is stored personal information regarding at least one individual, which information comprises information regarding said individual's state of health. The system also comprises a safety device adapted to protect at least parts of the information against unauthorized access.

PRIOR ART

It is previously known to store medical records in a database where the responsible care provider stores specific information about the state of health of an individual. This information is accessible to the responsible nursing staff, and the individual him-/herself may be granted access to the information about him-/herself if this is asked for.

It is also known that an individual uses a so-called patient's card, a plastic card including name, personal code number and address data used in the care sector. It simplifies the administrative work for the nursing staff and minimizes the risk of personal data becoming incorrect. The patient's card is embossed free of charge at the patient information desk of the hospitals and is an important stage not only upon the admission but all through the "care chain".

Different care providing institutions with which an individual may get into contact use different systems to identify the individual and store information about the individual. Accordingly, in certain cases, an individual is identified by a patient's card and in other cases by some other kind of identification. The respective care provider uses its own databases to store medical records including information about the individual. This entails that different hospitals among themselves have different records about one and the same individual. Care providers in public as well as private medical services and other institutions that an individual is contacting, such as hospitals, dentists, care centres, optical and audiology clinics, opticians, pharmacies and different therapists, have all the their own systems to store information about their respective patients, where one and the same individual may be present in one or more of these different systems.

It should also be mentioned that different systems are known whereby the identity of a user or an individual can be established. These may roughly be divided into two categories, one category where the user or the individual carries something that can be used to show his/her identity, such as a magnetic card, a smart card, a bar-code, an RFID transmitter, an inductive transmitter, or a USB key, whereby it is possible to establish the identity of the carrier. Another category is that the user or the individual is identified by biometric information that is unique to the user or the individual.

SUMMARY OF THE PRESENT INVENTION

Problems

There is a technical problem to be able to afford integrated information about the state of health of an individual where a care provider can be given a complete picture of the actions of different care providers, which complete picture may be crucial to be able to afford adequate aid in a specific situation.

There is a technical problem to afford the individual a security that personal information is handled in a proper way, that the information only is accessible to authorized users, and that required information is accessible in case of special needs, such as upon acute illnesses or accidents when the individual maybe is not close to the care provider.

There is also a technical problem to afford access to general information about the state of health of an individual for a certain category of users, where this general information concerns information that is required to provide adequate help in public medical service or in connection with an acute situation, and to afford access to specific information for another category of users, where this specific information concerns confidential information regarding a specific health care action.

There is also a problem to be able to compile information of several individuals regarding their illnesses, the caring measures that have been taken to help the individual as well as the results achieved thereby, and make this information accessible to research and development or evaluation of caring actions carried out, as well as to do this in a way so that the individual's integrity is not violated. There is also a technical problem to make accessible such

information in a simple and efficient way when it is still new so that fresh information can be made accessible to research and development.

There is a problem to prevent abuse or unauthorized access to the information, as well as to prevent anyone from changing, deleting or adding information about an individual without this being made in a way so that the individual or authorized users can view what has been made, when it was made, and who made it.

There is a problem to allow the individual to get access in a simple way to the general as well as the specific information that has been stored regarding him-/herself, and simultaneously to prevent said individual from altering the information about him-/herself in an undue way.

There is also a problem to make accessible the information to a user in several different places, such as at various care institutions or even outside in the field at scenes of accidents or emergency areas.

There is a technical problem to make the information accessible to a user that does not know the individual if the individual is not contactable, such as at a scene of an accident where an individual is found and is unconscious.

Solution

With the purpose of solving one or several of the above problems, and on the basis of prior art such as it has been shown above and the indicated technical field, the present invention teaches that a database according to the invention is divided into a first storage space and a second storage space, and that the safety device is adapted to grant an authorized user access to the first storage space according to a first safety level and to the second storage space according to a second safety level.

In the first storage space, there is stored general information about the individual's state of health, and in the second storage space, there is stored specific information about the individual's state of health. The safety device is adapted to demand a first authorization key belonging to the individual in combination with a second authorization key belonging to the authorized user in order for access to the first storage space to be granted to the authorized user.

When all information about the individual is integrated in a common database, an authorized user can accordingly be granted access to a general

picture of the different care actions the individual has been subjected to, which may be crucial to how continued care should be offered in a way that is best for the individual.

The present invention teaches that the general information concerns information that is required to provide adequate help in an acute situation, such as the individual's personal data, blood group, diseases that may require fast actions, mental or physical handicap, heart disease, diabetes, allergies, epilepsy, impaired vision and/or hearing as well as vitally important medication, and that the first safety level is adapted to grant an authorized user from public or private medical service or immediate assistance corps, such as staff from the rescue services agency, ambulance services, fire fighting services, police force, pharmacies, dentists, opticians, receptions in emergency wards, optical and audiology clinics, care institutions and primary care, access to this general information.

This solves the existing problems of being able to take into consideration the general condition of an individual in connection with an acute situation or of easily being able to get a comprehensive picture of the individual's general state of health when the individual gets into contact with public medical service.

The present invention teaches further that the specific information concerns confidential information regarding a specific health care action, and that the second safety level is adapted to grant registered staff in the care sector access to specific information about the individual regarding the special action this very user works with, where registered staff, for instance, may be caring staff such as a physician, a nurse, a dentist, an optician, or a registered therapist. Registered staff may also consist of non-nursing staff that still may need access to data in the specific information, such as an officer at the regional social insurance office.

An authorized user may also consist of person or a company that has got admission or commission from the individual, such as an insurance company or physician that works in an insurance company.

With the intention to afford access to integrated information about several individuals' illnesses, the caring measures that have been taken to help the individual as well as the results achieved thereby, the present invention teaches that the information in the inventive system can be made accessible in anonymous form regarding the individual's identity in other contexts than in caring actions of

the individual, such as for research and development, statistical compilations or for evaluation of medicines, methods of treatment, or other caring actions.

With the purpose of securely establishing that the information in the database is not incorrectly changed or deleted, or that information is incorrectly added, the present invention teaches that the safety device is adapted to determine a first degree of authorization, which is adapted to give an authorized user an authorization to read information from the database, a second degree of authorization, which is adapted to give an authorized user authorization to write information to the database, as well as a third degree of authorization, which is adapted to give an authorized user authorization to remove information from the database, and that an authorized user can be assigned access to the information in the database according to a suitable combination of the first and second safety level and the first, second and third degree of authorization, respectively.

With the intention to afford a possibility of viewing who has made changes in the information, when changes were made and what changes were being made, the present invention teaches that the system comprises a log, and that each access of the database, and each action taken upon such an access, is recorded in the log together with the user's identity as well as the instant of time of the access.

In order to give an individual the possibility of viewing which information is stored regarding him-/herself, the present invention teaches that the safety device is adapted to grant the individual access to the first and second storage space by means of the first authorization key. Such an access for the individual is assigned at least according to the first degree of authorization, i.e., the right to read information.

The present invention teaches that the safety device comprises means for reading and checking the first and second authorization key.

An authorization key may consist of different items whereby an individual and a user can identify him-/herself. Accordingly, it comprises a means that is available to read and check the first and second authorization key, an interface for the communication with an authorization key, such as a keyset, a touch panel, a reader of magnetic cards or smart cards, a reader of bar-codes, an RFID receiver, an inductive receiver, or an interface for the communication with a USB key, and the first and/or second authorization key may accordingly consist of something an

individual or a user possesses, such as a personal code, a magnetic card, a smart card, a bar-code, an RFID transmitter, an inductive transmitter, or a USB key.

According to the present invention, it is also possible that the means that is available to read and check the first and second authorization key comprises an interface for the reading of biometric information and the provision of biometric identification, such as a reader of finger prints, hand prints, eye recognition, ear recognition, face recognition, or voice recognition, and that the first and/or second authorization key are/is a biometrically unique feature belonging to the individual or the user.

Another type of biological unique information is the DNA of an individual, which in certain cases, such as in accidents or catastrophes, may be the only way of identifying an individual, so it is possible that the means that is available to read and check the first authorization key comprises analysis tools for DNA, and that the first authorization key is the individual's DNA.

With the purpose of making accessible the information of the database in several different and geographically scattered places, the present invention teaches that the safety device comprises a plurality of different means, which means are distributed and geographically placed to be easily accessible to different authorized users.

It is also possible that the safety device comprises means that are mobile, and that these means are adapted to be carried in emergency vehicles or rescue vehicles to be usable at scenes of accidents or emergency areas and in such a way grant access to information about individuals that may need help directly on a scene of an accident.

With the intention to afford a possibility of giving an authorized user access to the general information in a situation where it is difficult or impossible to establish communication with the database, the present invention teaches that the means may comprise a third storage space, and that a copy of the general information stored in the first storage space and belonging to the respective individual is stored in the third storage space.

This makes it possible to grant an authorized user access to the general information via the third storage space in a situation where it is difficult or impossible to establish communication with the database.

In order to afford a possibility of keeping the third storage space updated, the present invention teaches that the third storage space is adapted to be synchronized with the first storage space upon a contact between the means and the database.

With the intention to afford a further possibility of giving an authorized user access to the general information in a situation where it is difficult or impossible to establish communication with the database, the present invention teaches that the first authorization key is a physical unit, which comprises a fourth storage space, and that a copy of the general information stored in the first storage space and belonging to the individual is stored in the fourth storage space. This makes it possible for a user to get access to the general information without therefore communicating with the database, since this information is accessible via the fourth storage space.

In order to afford a possibility of keeping the fourth storage space updated, the present invention teaches that the fourth storage space is adapted to be synchronized with the first storage space upon a contact between the first authorization key and the database.

If the first authorization key is a physical unit, it is also possible to allow the same to comprise a position-indicating unit, such as a GPS receiver, as well as a transmitting unit, and that the physical unit is adapted to send out a signal that indicates the position of the physical unit, via the position-indicating unit and the transmitting unit, in an emergency situation.

It is also suggested that the physical unit may comprise a receiving unit, and that the position-indicating unit as well as the transmitting unit is adapted to be activated when the receiving unit receives an activating signal.

The first authorization key should preferably be carried by the individual all the time, and the present invention teaches different kinds of first authorization keys that easily are brought and carried by the individual without major effort. In the same way, it may be important that also the second authorization key easily can be carried by a user.

Accordingly, the present invention teaches that the first and/or second authorization key are/is inserted by operation in the individual's or the user's body.

It is also possible that the first and/or second authorization key are/is a piece of jewellery or, for instance, a tattoo.

Advantages

The advantages that foremost may be associated with a system according to the present invention are that the system according to the invention affords integrated information about the state of health of an individual, which means that a care provider can be granted access to crucial information that is required to be able to provide a correct caring action.

Even if the information is integrated, the system only allows that authorized users are granted access to the information, and different users can be given different authorization so that only required information should be accessible to the respective user.

The integrated information may also be made accessible in anonymous form for research and development as well as evaluation of caring actions or medicines, which brings an enormous advantage as an integrated amount of information of a large number of individuals from a large number of care providers having fresh information is made accessible instantaneously, which information is continuously updated when the individuals receive caring actions in various ways.

The general information is accessible everywhere where means for reading the individual's authorization key are available, which means that also in acute situations at scenes of accidents or emergency areas, ambulance service staff or rescue services staff can be granted access to essential information about the medical background and health of the victims, and this even if the individual is unconscious. Accordingly, the present invention can save lives by crucial information being easily accessible in critical situations.

A further advantage is that the present invention gives the possibility of fast and easily identifying deceased individuals by reading the individual's authorization key.

The present invention also grants the individual access to his/her own stored information, which gives a possibility of his/her own checking of the information to avoid mistake and prevent errors.

The present invention also affords the individual a freedom to make his/her own choice of care provider and still know that this care provider has access to possible information of earlier care actions as well as information about

the current state of health as the basis for the care actions that should be carried out.

By the present invention, a possibility of compiling a historical account of the medical and care record of an individual is afforded. Accordingly a historical account of, for instance, the individual's vaccinations may be readily compiled. It is also possible to compile other historical accounts, such as the accumulated exposure to x-rays of an individual or an accumulated intake of a medical preparation.

BRIEF DESCRIPTION OF THE DRAWINGS

A system having the properties associated with the present invention will now be described in more detail for the purpose of exemplifying, reference being made to the accompanying drawing, wherein:

Figure 1 shows schematically a system according to the invention,

Figure 2 shows schematically a system having distributed means for the reading and checking of authorization keys, and

Figure 3 shows schematically an alternative embodiment of a first authorization key.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following, the present invention will be described with a reference to Figure 1 showing a system 1 comprising a database 11 in which personal information 12 regarding at least one individual A is stored, where the information 12 comprises information regarding the individual A's state of health.

It should be appreciated that even if the present invention in the following many times will be described with an individual A, the invention is adapted to handle information related to a large number of individuals where the advantages of the invention increase with the number of individuals and where the number of individuals only is limited by the size of accessible storage spaces in the database and the capacity of the database management used of handling great amounts of information.

A system 1 according to the present invention also comprises a safety device 13 adapted to protect at least parts of the information 12 against unauthorized access.

The present invention teaches particularly that the database 11 is divided into a first storage space 14 and a second storage space 15, and that the safety device 13 is adapted to grant an authorized user B access to the first storage space 14 according to a first safety level and to the second storage space 15 according to a second safety level.

It should be appreciated that even if the present invention in the following many times will be described with a user B, the invention is adapted to handle a large number of users and their respective authorizations where the advantages of the invention can be considered to increase with the number of users.

In the first storage space 14, there is stored general information 12a about the individual A's state of health, and in the second storage space 15, there is stored specific information 12b about the individual A's state of health. The safety device 13 is adapted to demand a first authorization key 16 belonging to the individual A in combination with a second authorization key 17 belonging to the authorized user B in order for access to the first storage space 14 to be granted to the authorized user B.

The general information 12a concerns information that is required to provide adequate help in an acute situation. Such information may be the individual A's personal data, blood group, diseases that may require fast actions, mental or physical handicap, heart disease, diabetes, allergies, epilepsy, impaired vision and/or hearing as well as vitally important medication. The first safety level is adapted to grant an authorized user B from public medical service or immediate assistance corps, such as staff from the rescue services agency, ambulance services, fire fighting services, police force, pharmacies, dentists, opticians, receptions in emergency wards, optical and audiology clinics, care institutions and primary care, access to the general information 12a.

The specific information 12b concerns confidential information regarding a specific health care action, and the second safety level is adapted to grant users B, which are registered staff in the care sector, access to specific information about the individual regarding the special action this very user works with, where registered staff, for instance, may be a physician, a nurse, a dentist, an optician, a registered therapist, a pharmacist, or an officer at the regional social insurance office.

It should be appreciated that different users may, according to his/her respective authorization, be granted access to different parts of the general information 12a and the specific information 12b, the information 12 is accordingly selectively accessible according to authorization. For instance, a pharmacist can only read prescriptions but is not granted access to the entire case sheet of an individual. Officers at, for instance, an insurance company have only access to information requisite for them. A physician may be given further authorization to be able to view information regarding other users' caring actions, thereby being able to adapt his/her own action to what has been made in other circumstances.

It should be appreciated that the present invention is not limited to how "registered staff" is defined, since the one who is to be considered to be a user that should get access to the system according to the invention may vary from country to country depending on local legislation. In some countries, complementary or alternative forms of treatment are accepted, and therapists that act within these forms of treatment may then, for instance, be registered staff. The important thing is to protect the individuals' integrity by the information only being made accessible to users that ought to have access to it.

The present invention teaches that an authorized user B also may be person or a company that has got admission or commission from the individual A, such as an insurance company or physician that works in an insurance company.

According to a proposed embodiment, it is possible to make accessible the information 12 in anonymous form 12' regarding the individual's identity, i.e., the information about the individuals is accessible but without the respective individual can be identified and associated with the information. Such anonymous information 12' may be very valuable in other contexts than in caring actions of the individual A, such as for research and development, statistical compilations or for evaluation of medicines, methods of treatment, or other caring actions, particularly since the information 12 and accordingly also the anonymous information 12' is updated continuously in connection with the individuals' contact with different medical care institutions, which makes that new and fresh information is made directly accessible in anonymous form 12' for research and development, statistical compilations and evaluations.

It is suggested that the safety device 13 is adapted to determine a first degree of authorization, which is adapted to give an authorized user B an

authorization to read information from the database 11, a second degree of authorization, which is adapted to give an authorized user B authorization to write information to the database 11, as well as a third degree of authorization, which is adapted to give an authorized user B authorization to remove information from the database 11, and the safety device 13 is adapted to assign an authorized user B access to the information 12 in the database 11 according to a suitable combination of the first and second safety level and the first, second and third degree of authorization, respectively.

The present invention teaches that the system 1 comprises a log 18, in which each access of the database 11, and each action taken upon such an access, is recorded together with the user B's identity as well as the instant of time of the access.

It is possible to adapt the safety device 13 to grant the individual A access to the first and second storage space 14, 15 by means of the first authorization key 16, in which way the individual him-/herself can get access to the information available about him/her.

Such an access is assigned at least according to the first degree of authorization, i.e., the authorization to read information. Such an access can, for instance, be used to allow the individual A to get reminded about medication, vaccinations or next visit to medical care.

If the individual A also is granted access to the database 11 according to the second degree of authorization, i.e., the authorization to write information, such an access and authorization may, for instance, be used to allow the individual A to make his/her own notes about his/her state of health and accordingly create a historical account of his/her state of health, where a user B at a later stage can be granted access to such personal notes made by the individual A.

The present invention teaches that the safety device 13 comprises means 2 to read and check the first and second authorization key 16, 17.

Such means 2 comprises an interface 2a for the communication with an authorization key 16, 17.

Such an interface 2a may be a keyset, a touch panel, a reader of magnetic cards or smart cards, a reader of bar-codes, an RFID receiver, an inductive receiver, or an interface for the communication with a USB key.

Accordingly, the first and/or second authorization key 16, 17 may consist of something an individual A or user B possesses and that can be used to communicate with a means 2 according to the invention. Hence, an authorization key 16, 17 may, for instance, be a personal code, a magnetic card, a smart card, a bar-code, an RFID transmitter, an inductive transmitter, or a USB key.

It is also possible that a means 2 according to the invention comprises an interface 2a for the reading of biometric information and the provision of biometric identification, such as a reader of finger prints, hand prints, eye recognition, ear recognition, face recognition, or voice recognition, and that the first and/or second authorization key 16, 17 are/is a biometrically unique feature belonging to the individual A or the user B.

For instance, it is possible that the means 2 comprises analysis tools for DNA, and that the first authorization key is the individual's DNA.

It should be appreciated that a means 2 may comprise different interfaces whereby the means 2 can communicate with different types of authorization keys.

Figure 2 shows an embodiment where the safety device 13 comprises a plurality of different means 21, 22, 23, ..., 2n, which may be distributed and geographically placed to be easily accessible to the authorized user B. These means may be mutually different regarding interfaces 2a for the communication with an authorization key to allow a communication with different types of authorization keys.

The distributed means 21, 22, 23, ..., 2n may be adapted to communicate with the database 11 in various ways. One part may communicate via connection to the Internet 3, others may communicate via local networks, telecommunication, radio communication or in other ways. The invention is not limited to how the different distributed means 21, 22, 23, .., 2n communicate with the database 11.

It should also be mentioned that a means 23 according to the invention may be mobile, where the means 23 is adapted to be carried in an emergency vehicle or rescue vehicle 4 in order to be accessible and useable at scenes of accidents or emergency areas.

It is suggested that the means 23 may comprise a third storage space 5, and that a copy 12a' of the general information 12a stored in the first storage space 14 and belonging to the respective individual A is stored in the third storage space 5.

This means that an authorized user B can be granted access to the copy 12a' of the general information 12a via the third storage space 5 in a situation where it is difficult or impossible to establish communication with the database 11, which may be the case at inaccessible scenes of accidents or in connection with natural disasters. When the copy 12a' of the general information 12a is accessible locally, authorized users B can still gain access to the general information 12a of an individual by the individual's first authorization key 16 and the user's second authorization key 17 in spite of the circumstances maybe making that no communication can be established with the database 11.

It is suggested that the third storage space 5 is adapted to be synchronized with the first storage space 14 upon a contact between the means 23 and the database 11.

In order to further ensure that the general information 12a is accessible without depending on connection to the database 11, it is suggested that if the first authorization key 16 is a physical unit, the same may comprise a fourth storage space 6, in which a copy 12a" of the general information 12a stored in the first storage space 14 and belonging to the individual A is stored.

An authorized user B may then be granted access to the copy 12a" of the general information 12a via the fourth storage space 6 in a situation where it is difficult or impossible to establish communication with the database 11.

The fourth storage space 6 may be adapted to be synchronized with the first storage space 14 upon a contact between the first authorization key 16 and the database 11.

Figure 3 shows an embodiment where the first authorization key 16 is a physical unit 16' that comprises a position-indicating unit 7, such as a GPS receiver, as well as a transmitting unit 8. The physical unit 16' may be adapted to, in an emergency situation, send out a signal that indicates the position of the physical unit 16' via the position-indicating unit 7 and the transmitting unit 8.

Such a physical unit 16' can be used to find individuals A that are searched for in connection with greater accidents, earthquakes, avalanches, or other natural disasters. It may also be used to find an individual A that is lost and searched for.

In order to further allow the searching of a missing individual A, the present invention teaches that the physical unit 16' comprises a receiving unit 9,

and that the position-indicating unit 7 as well as the transmitting unit 8 are adapted to be activated when said receiving unit 9 receives an activating signal, which makes it possible to activate the position-providing unit 7 and the transmitting unit 8 by sending an activating signal to the receiving unit 9 should it be that the user A not by him-/herself is able to activate the position-providing unit 7 and the transmitting unit 8.

It should be appreciated that the embodiments described above having a physical authorization key can be combined arbitrarily. Accordingly, it is possible to afford a physical authorization key having a fourth storage space 6 but without a position-indicating unit 7, it is also possible to afford a physical unit having a position-indicating unit 7 but without a fourth storage space 6, and it is naturally also possible to afford a physical unit having a fourth storage space 6 as well as a position-indicating unit 7.

There are different ways to carry an authorization key 16, 17, and in order for the individual A or the user B always to be able to carry his/her authorization key 16, 17, the present invention teaches that the first and/or second authorization key 16, 17 may be inserted by operation in the individual A's or the user B's body.

It is also possible that the first and/or second authorization key 16, 17 are/is a piece of jewellery or a tattoo.

The invention is of course not limited to the embodiments given above as examples but may be subjected to modifications within the scope of the general idea according to the invention such as this is shown in the subsequent claims.

CLAIMS

1. System comprising a database, where in the database, there is stored personal information regarding at least one individual, where said information comprises information regarding said individual's state of health, as well as a safety device adapted to protect at least parts of said information against unauthorized access, **characterized in** that said database is divided into a first storage space and a second storage space, that said safety device is adapted to grant an authorized user access to said first storage space according to a first safety level and to said second storage space according to a second safety level, that in said first storage space, there is stored general information about said individual's state of health, that in said second storage space, there is stored specific information about said individual's state of health, that said safety device is adapted to demand a first authorization key belonging to said individual in combination with a second authorization key belonging to said authorized user in order for access to said first storage space to be granted to said authorized user, that said general information concerns information that is required to provide adequate help in an acute situation, and that said first safety level is adapted to grant an authorized user from public medical service or immediate assistance corps access to said general information, and that said specific information concerns confidential information regarding a specific health care action, and that said second safety level is adapted to grant registered staff in the care sector access to specific information about said individual regarding the special action this very user works with.

2. System according to claim 1, **characterized in** that an authorized user may be person or a company that has got admission or commission from said individual.

3. System according to any one of the preceding claims, **characterized in** that said information in anonymous form regarding the individual's identity is made accessible in other contexts than in caring actions of the individual.

4. System according to any one of the preceding claims, **characterized in** that said safety device is adapted to determine a first degree of authorization, which is adapted to give an authorized user an authorization to read information from said database, a second degree of authorization, which is adapted to give an authorized user authorization to write information to said database, as well as a third degree of authorization, which is adapted to give an authorized user authorization to remove information from said database, and that an authorized user can be assigned access to the information in said database according to a suitable combination of said first and second safety level and said first, second and third degree, respectively, of authorization.

5. System according to any one of the preceding claims, **characterized in** that said system comprises a log, and that each access of said database, and each action taken upon such an access, is recorded in said log together with said user's identity as well as the instant of time of the access.

6. System according to any one of the preceding claims, **characterized in** that said safety device is adapted to grant said individual access to said first and second storage space by means of said first authorization key.

7. System according to the claims 4 and 6, **characterized in** that said access is assigned at least according to said first degree of authorization.

8. System according to any one of the preceding claims, **characterized in** that said safety device comprises means for reading and checking said first and second authorization key.

9. System according to claim 8, **characterized in** that said means comprises an interface for the communication with an authorization key, and that said first and/or second authorization key are/is something an individual or a user possesses.

10. System according to claim 8 or 9, **characterized in** that said means comprises an interface for the reading of biometric information and the provision of

biometric identification, and that said first and/or second authorization key are/is a biometrically unique feature belonging to said individual or user.

11. System according to claim 8, 9 or 10, **characterized in** that said means comprises analysis tools for DNA, and that said first authorization key is said individual's DNA.

12. System according to any one of claims 8 to 11, **characterized in** that said safety device comprises a plurality of different means, and that said means are distributed and geographically placed to be easily accessible to said authorized user.

13. System according to claim 12, **characterized in** that said means is mobile, and that said means is adapted to be carried in emergency vehicles or rescue vehicles.

14. System according to claim 12 or 13, **characterized in** that said means comprises a third storage space, and that a copy of the general information stored in said first storage space and belonging to the respective individual is stored in said third storage space.

15. System according to claim 14, **characterized in** that an authorized user can be granted access to said general information via said third storage space in a situation where it is difficult or impossible to establish communication with said database.

16. System according to claim 14, **characterized in** that said third storage space is adapted to be synchronized with said first storage space upon a contact between said means and said database.

17. System according to claim 9, **characterized in** that said first authorization key is a physical unit, that said physical unit comprises a fourth storage space, and that a copy of the general information stored in said first storage space and belonging to said individual is stored in said fourth storage space.

18. System according to claim 17, **characterized in** that an authorized user can be granted access to said general information via said fourth storage space in a situation where it is difficult or impossible to establish communication with said database.

19. System according to claim 17, **characterized in** that said fourth storage space is adapted to be synchronized with said first storage space upon a contact between said first authorization key and said database.

20. System according to claim 9 or 17, **characterized in** that said first authorization key is a physical unit, that said physical unit comprises a position-indicating unit, as well as a transmitting unit, and that said physical unit is adapted to send out a signal that indicates the position of said physical unit, via said position-indicating unit and said transmitting unit, in an emergency situation.

21. System according to claim 20, **characterized in** that said physical unit comprises a receiving unit, and that said position-indicating unit as well as transmitting unit is adapted to be activated when said receiving unit receives an activating signal.

22. System according to claim 9, 17, 20 or 21, **characterized in** that said first and/or second authorization key are/is inserted by operation in said individual's or user's body.

23. System according to claim 9, 17, 20 or 21, **characterized in** that said first and/or second authorization key are/is a piece of jewellery.

24. System according to claim 9, **characterized in** that said first and/or second authorization key are/is a tattoo.

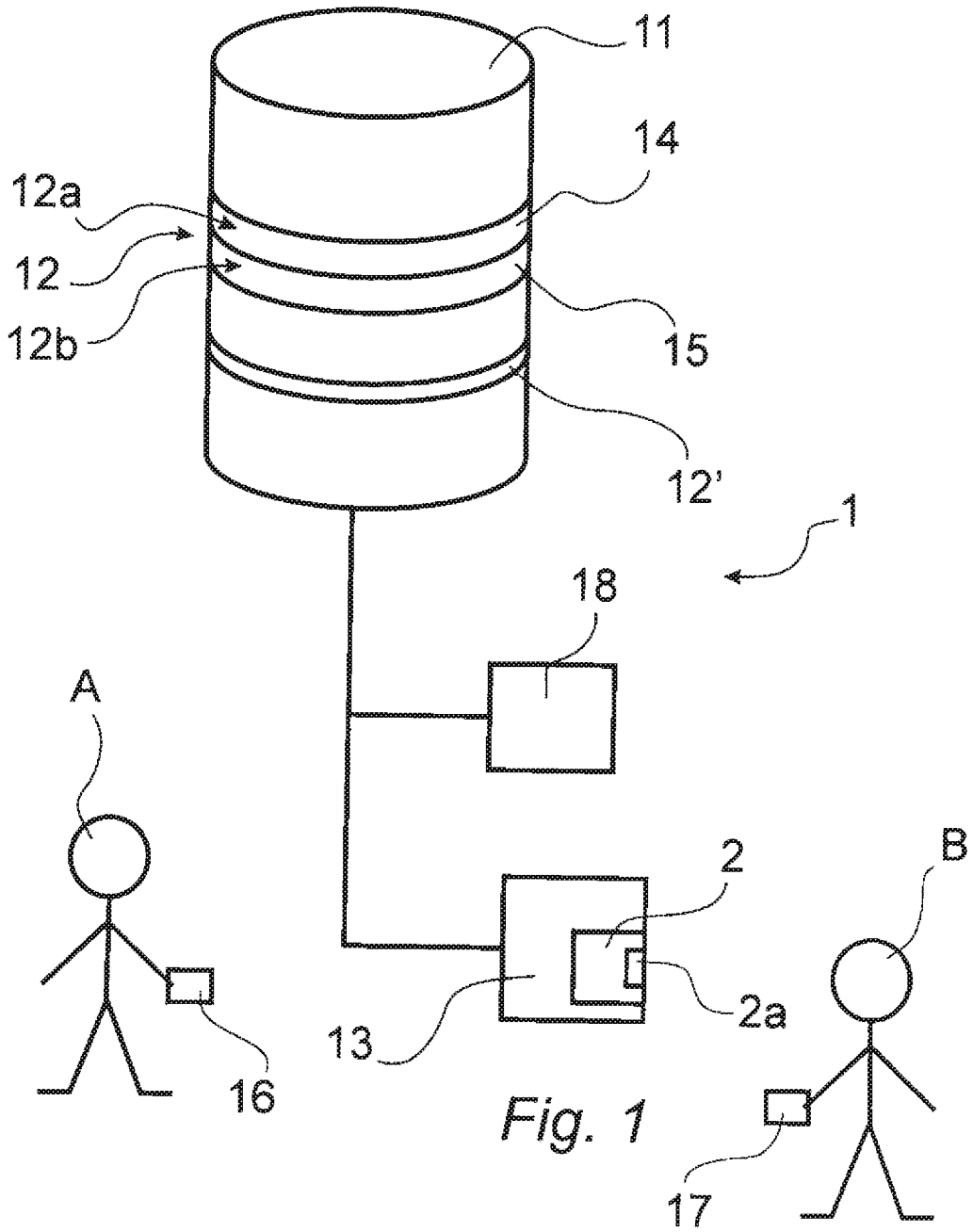

Fig. 1

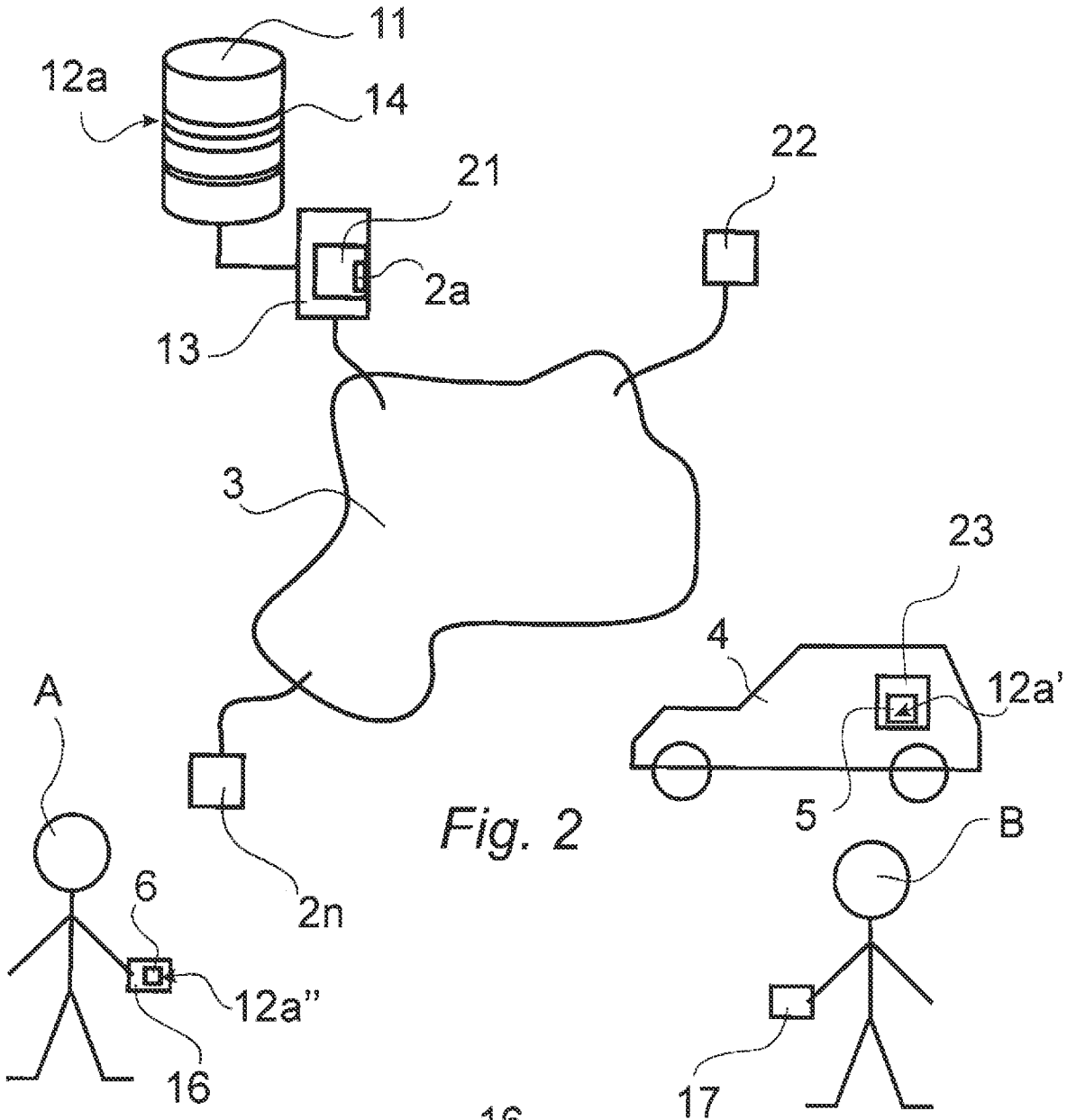

Fig. 2

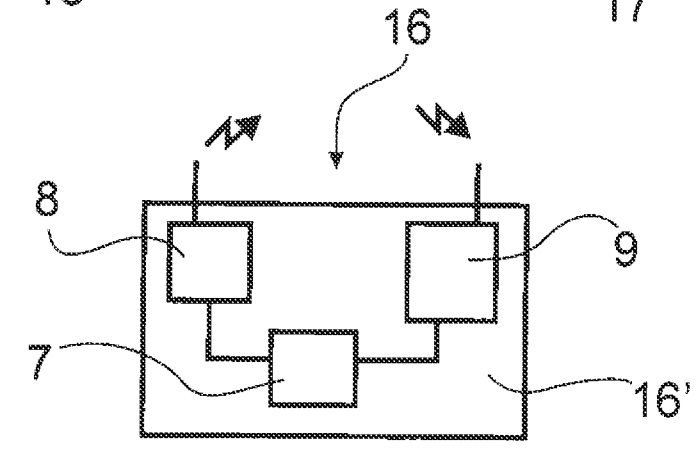

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2010/051307

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F, G06Q, A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006019623 A2 (MEDTRONIC MINIMED, INC.), 23 February 2006 (23.02.2006), abstract, paragraphs (0056)-(0057), (0059), (0083), (0112)-(0113)	1-24
	--	
Y	US 20080262868 A1 (A. MALOLEPSZY), 23 October 2008 (23.10.2008), claim 2, paragraphs (0013), (0023), (0031)-(0033)	1-24
	--	
Y	US 20080027752 A1 (G.T. PHAN ET AL), 31 January 2008 (31.01.2008), abstract, paragraphs (0021), (0035)	1-24
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February 2011	28-02-2011
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christian Wall / JA A Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2010/051307

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2008043341 A1 (INFOKOM GMBH), 17 April 2008 (17.04.2008), abstract ---	1-24
A	WO 2009071194 A1 (ROCHE DIAGNOSTICS GMBH), 11 June 2009 (11.06.2009), figure 1, abstract ---	1-24
A	WO 0171469 A1 (DAHMS, J.W.), 27 Sept 2001 (27.09.2001), abstract --- --------	1-24

International patent classification (IPC)

G06F 17/30 (2006.01)
G06F 21/00 (2006.01)
G06Q 50/00 (2006.01)
A61B 5/00 (2006.01)

Download your patent documents at www.prv.se

The cited patent documents can be downloaded:

- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **TCNZGTDWBQ**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE2010/051307

WO	2006019623	A2	23/02/2006	CA	2573438	A	23/02/2006
				EP	1793729	A	13/06/2007
				JP	2008508934	T	27/03/2008
				US	20060031094	A	09/02/2006
US	20080262868	A1	23/10/2008	NONE			
US	20080027752	A1	31/01/2008	NONE			
WO	2008043341	A1	17/04/2008	DE	102006048110	A	17/04/2008
				DE	112007003101	A	17/09/2009
WO	2009071194	A1	11/06/2009	US	20090150174	A	11/06/2009
WO	0171469	A1	27/09/2001	AU	4924001	A	03/10/2001