

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 June 2007 (21.06.2007)

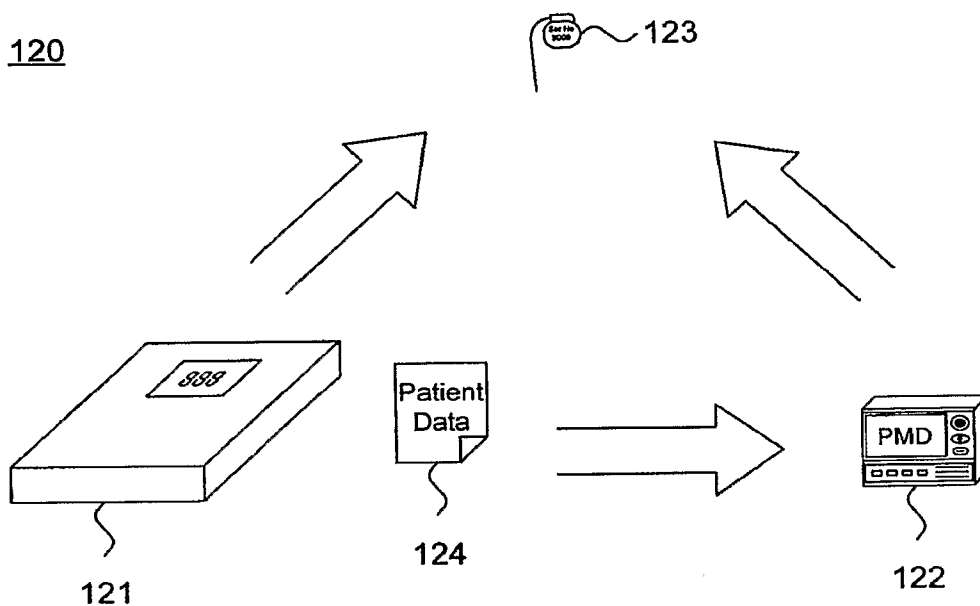
PCT

(10) International Publication Number
WO 2007/070551 A2

- (51) International Patent Classification:
A61B 5/00 (2006.01) A61B 5/117 (2006.01)
 - (21) International Application Number:
PCT/US2006/047485
 - (22) International Filing Date:
11 December 2006 (11.12.2006)
 - (25) Filing Language: English
 - (26) Publication Language: English
 - (30) Priority Data:
11/301,214 12 December 2005 (12.12.2005) US
 - (71) Applicant (for all designated States except US): **CARDIAC PACEMAKERS, INC.** [US/US]; 4100 Hamline Avenue North, St. Paul, Minnesota 55112-5798 (US).
 - (72) Inventors; and
 - (75) Inventors/Applicants (for US only): **DONG, Yanting** [CN/US]; 295 Oakhill Drive, Shoreview, Minnesota 55126 (US). **CARPENTER, Todd P.** [US/US]; 885 S. Lexington Pkwy, St. Paul, Minnesota 55116-2366 (US). **NI, Quan** [CN/US]; 5812 Prairie Ridge Drive, Shoreview, Minnesota 55126 (US). **HOYME, Kenneth P.** [US/US]; 5930 Annapolis Lane North, Plymouth, Minnesota 55446 (US).
 - (74) Agent: **INOUYE, Patrick Joseph Sus**; 500 Union Street, Ste 1005, Seattle, WA 98101 (US).
 - (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: PROVIDING AUTHENTICATION OF REMOTELY COLLECTED EXTERNAL SENSOR MEASURES



(57) Abstract: A system (10) and method (30) for providing authentication of remotely collected external sensor (17) measures is presented. Physiological measures (37) are collected (31) from a source (17) situated remotely from a repository (18) for accumulating such collected physiological measures (37). An identification (32) of the source from which the physiological measures (37) were collected (31) is determined against authentication data (82) that uniquely identifies a specific patient (14). The physiological measures (37) are forwarded (33) to the repository upon authenticating the patient identification (80) as originating from the specific patient (14).

WO 2007/070551 A2



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PROVIDING AUTHENTICATION OF REMOTELY COLLECTED EXTERNAL SENSOR MEASURES

TECHNICAL FIELD

The present invention relates in general to external sensor authentication and, specifically, to a system and method for providing authentication of remotely collected external sensor measures.

BACKGROUND ART

Remote patient management has become increasingly attractive as an alternative to routine clinical follow-up in light of trending increases in healthcare costs. Remote patient management enables a clinician, such as a physician, nurse, or other healthcare provider, to follow patient well-being through homecare medical devices that can collect and forward patient data without requiring the presence or assistance of medical personnel. Advances in automation have encouraged such self-care solutions and public data communications networks, in particular, the Internet, have made ready data retrieval and patient communication viable and widely available.

To participate in remote patient management, each patient installs an at-home medical device, such as a patient management device, for collecting quantitative patient data measured by external sensors, such as a weight scale, blood pressure cuff, pulse oximeter, or glucometer, and for connecting to a centralized patient management facility, frequently implemented as a server accessible over the Internet. Other devices, such as a personal computer, can measure and report qualitative patient data. In addition, implantable medical devices (IMDs), for example, pacemakers and implantable defibrillators, are beginning to include the capability to work with at-home medical devices.

To succeed, remote patient management must be user-friendly to encourage regular use. Difficulties in use will discourage patients and decrease the effectiveness of treatment and the benefit received. Ideally, remote patient management devices should introduce no more than minimal inconvenience, such as experienced when using a bathroom scale or thermometer, and will accommodate the needs of the infirm, elderly and physically challenged. Additionally, these devices should transparently manage spurious data, such as resulting from unauthorized use and from use by sources other than the patient, because raw patient data cannot easily be associated

with a specific authorized patient. Conventional remote patient management devices assume that the patient is the only user and rely on implicit patient identification.

U.S. Patent No. 6,168,563, to Brown, discloses a system and method that enables a healthcare provider to monitor and manage a health condition of a patient. A clearinghouse
5 computer communicates with the patient through a data management unit, which interactively monitors the patient's health condition by asking questions and receiving answers that are supplied back to the clearinghouse computer. Patient information may also be supplied by physiological monitoring devices, such as a blood glucose monitor or peak-flow meter. Healthcare professionals can access the patient information through the clearinghouse computer,
10 which can process, analyze, print, and display the data. However, Brown fails to disclose specific controls to ensure proper patient identification prior to accepting data from the data management unit.

U.S. Patent No. 6,416,471, to Kumar et al. ("Kumar"), discloses a portable remote patient telemonitoring device. A disposable sensor band with electro-patches detects and transmits vital
15 signs data to a signal transfer unit, which can be either be worn or positioned nearby the patient. The base station receives data transmissions from the signal transfer unit for transferring the collected data to a remote monitoring station. Indications are provided to a patient from a base station when threshold violations occur. However, Kumar fails to disclose authenticating the identity of the patient prior to receiving collected data from the base station.

U.S. Patent No. 6,024,699, to Surwit et al. ("Surwit"), discloses a central data processing
20 system configured to communicate with and receive data from patient monitoring systems, which may implement medical dosage algorithms to generate dosage recommendations. Blood from a pricked finger may be read on a chemically treated strip for review at the central data processing system. Modifications to medicine dosages, the medicine dosage algorithms, patient
25 fixed or contingent self-monitoring schedules, and other treatment information are communicated. However, Surwit fails to disclose identifying the patient submitting the sample through each patient monitoring system.

Therefore, there is a need for providing an automated determination of patient
30 identification associated with patient data collected by remote external and unsupervised sensors to ensure the integrity of the data received. Preferably, such an approach would provide a range of patient authentication mechanisms customizable to meet patient needs and monitoring situations.

DISCLOSURE OF THE INVENTION

A system and method includes passive and active authentication of patient data received or accepted from a source under remote patient management. Active authentication requires a patient to undertake a physical action, such as providing biometric, token, or code entry
5 identifiers, which can provide identification credentials for comparison to authentication data prior to forwarding. Passive authentication utilizes credentialing indicia generally provided as an implantable device, such as an implantable medical device, implantable sensor, or implantable identification tag, to authenticate the physical proximity of a patient as the source of the patient data.

10 One embodiment provides a system and method for authenticating remotely collected external sensor measures. Physiological measures are collected from a source situated remotely from a repository for accumulating the physiological measures. The source of the physiological measures is identified by comparison to authentication data that uniquely identifies a specific patient. The physiological measures are forwarded to the repository upon authenticating the
15 patient data as originating from the specific patient.

Still other embodiments of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein are described embodiments of the invention by way of illustrating the best mode contemplated for carrying out the invention. As will be realized, the invention is capable of other and different embodiments and its several
20 details are capable of modifications in various obvious respects, all without departing from the spirit and the scope of the present invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a functional block diagram showing, by way of example, an automated
25 patient management environment.

FIGURE 2 is a process flow diagram showing a method for providing authentication of remotely collected external sensor measures, in accordance with one embodiment.

FIGURE 3 is a block diagram showing, by way of example, patient identification through passive authentication.

30 FIGURE 4 is a block diagram showing, by way of example, patient identification through active authentication.

FIGURE 5 is a functional block diagram showing patient identification with an external sensor.

FIGURE 6 is a flow diagram showing patient identification with an external sensor.

FIGURE 7 is a functional block diagram showing patient identification with a patient management device.

FIGURE 8 is a flow diagram showing patient identification with a patient management device.

5 FIGURES 9, 11, and 13 are functional block diagrams showing patient identification with an implantable medical device.

FIGURES 10, 12, and 14 are flow diagrams showing patient identification with an implantable medical device.

10 FIGURES 15 and 16 are functional block diagrams showing patient identification for multiple patients, in accordance with one embodiment.

BEST MODE FOR CARRYING OUT THE INVENTION

Automated patient management encompasses a range of activities, including remote patient management and automatic diagnosis of patient health, such as described in commonly-assigned U.S. Patent application Pub. No. US2004/0103001, published May 27, 2004, pending, 15 the disclosure of which is incorporated by reference. Such activities can be performed proximal to a patient, such as in the patient's home or office, centrally through a centralized server, such from a hospital, clinic or physician's office, or through a remote workstation, such as a secure wireless mobile computing device. FIGURE 1 is a functional block diagram showing, by way of example, an automated patient management environment 10. In one embodiment, a patient 14 is 20 proximal to one or more patient monitoring or communications devices, such as a patient management device 12, which are interconnected remotely to a centralized server 13 over an internetwork 11, such as the Internet, or through a public telephone exchange (not shown), such as a conventional or mobile telephone network. Other patient monitoring or communications devices are possible. In addition, the functionality provided by the centralized server 13 could 25 also be provided by local or decentralized servers, or by workstations, personal computers, or other computational systems accessible via the internetwork 11 or other form of network. The internetwork 11 can provide both conventional wired and wireless interconnectivity. In one embodiment, the internetwork 11 is based on the Transmission Control Protocol/Internet Protocol (TCP/IP) network communication specification, although other types or combination of 30 networking implementations are possible. Similarly, other network topologies and arrangements are possible.

Each patient management device 12 is uniquely assigned to a patient under treatment 14 to provide a localized and network-accessible interface to one or more medical devices 15-17, either through direct means, such as wired connectivity, or through indirect means, such as

selective radio frequency or wireless telemetry based on, for example, “strong” Bluetooth or IEEE 802.11 wireless fidelity “WiFi” and “WiMax” interfacing standards. Other configurations and combinations of patient data source interfacing are possible. Medical therapy devices include implantable medical devices (IMDs) 15, such as pacemakers, implantable cardiac defibrillators (ICDs), drug pumps, and neuro-stimulators, as well as external medical devices (not shown). Medical sensors include implantable sensors 16, such as implantable heart and respiratory monitors and implantable diagnostic multi-sensor non-therapeutic devices, and external sensors 17, such as Holter monitors, weight scales, and blood pressure cuffs. Other types of medical therapy, medical sensing, and measuring devices, both implantable and external, are possible.

Patient data includes physiological measures, which can be quantitative or qualitative, parametric data regarding the status and operational characteristics of the patient data source itself, and environmental parameters, such as the temperature or time of day. In a further embodiment, patient data can also include psychological, drug dosing, medical therapy, and insurance-related information, as well as other types and forms of information, such as digital imagery or sound and patient-provided or -uploaded information. The medical devices 15-17 collect and forward the patient data either as a primary or supplemental function. The medical devices 15-17 include, by way of example, implantable and external medical therapy devices that deliver or provide therapy to the patient 14, implantable and external medical sensors that sense physiological data in relation to the patient 14, and measurement devices that measure environmental parameters and other data occurring independent of the patient 14. Other types of patient data are possible. Each medical device 15-17 can generate one or more types of patient data and can incorporate one or more components for delivering therapy, sensing physiological data, measuring environmental parameters, or a combination of functionality.

Patient data received from IMDs 15 and implantable sensors 16 is known to have originated from a particular patient 14, as implantable devices are uniquely identified by serial number or other identifying data. Accordingly, any patient data originating from an implantable device can only be from the patient 14 in which the device was implanted. Patient data received from external sensors 17, however, is not uniquely tied to a particular patient 14 and could instead originate from another person, such as a spouse or family member, or random source, such as a pet that accidentally triggers a sensor reading. To ensure the integrity of patient data, the identification of the source from which the patient data was collected is confirmed against authentication data that uniquely identifies a specific patient 14 prior to being forwarded to the centralized server 13 or other patient data repository. In one embodiment, a patient data source

is associated with a specific patient in a one-to-one mapping that ensures authentication prior to receipt of the patient data at the centralized server 13, as further described below beginning with reference to FIGURE 2. Briefly, patient data is received or collected and the forwarding of the patient data to the centralized server 13 or, in a further embodiment, the patient management
5 device 12, is deferred until the identity of the source is locally authenticated through passive or active means. In a further embodiment, a single patient data source can be associated with multiple patients in a one-to-many mapping, such as further described below with reference to FIGURES 15 and 16.

In a further embodiment, data values can be directly entered by a patient 14. For
10 example, answers to health questions could be input into a personal computer with user interfacing means, such as a keyboard and display or microphone and speaker. Such patient-provided data values could also be collected as patient information. In one embodiment, the medical devices 15-17 collect the quantitative physiological measures on a substantially continuous or scheduled basis and also record the occurrence of events, such as therapy or
15 irregular readings. In a further embodiment, the patient management device 12, a personal computer, or similar device record or communicate qualitative quality of life (QOL) measures that reflect the subjective impression of physical well-being perceived by the patient 14 at a particular time. Other types of patient data collection, periodicity and storage are possible.

In a further embodiment, the collected patient data can also be accessed and analyzed by
20 one or more clients 19, either locally-configured or remotely-interconnected over the internetwork 11. The clients 19 can be used, for example, by clinicians to securely access stored patient data assembled in a database 18 and to select and prioritize patients for health care provisioning, such as respectively described in commonly-assigned U.S. Patent application, Serial No. 11/121,593, filed May 3, 2005, pending, and U.S. Patent application, Serial No.
25 11/121,594, filed May 3, 2005, pending, the disclosures of which are incorporated by reference. Although described herein with reference to physicians or clinicians, the entire discussion applies equally to organizations, including hospitals, clinics, and laboratories, and other individuals or interests, such as researchers, scientists, universities, and governmental agencies, seeking access to the patient data.

In a further embodiment, patient data is safeguarded against unauthorized disclosure to
30 third parties, including during collection, assembly, evaluation, transmission, and storage, to protect patient privacy and comply with recently enacted medical information privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the European Privacy Directive. At a minimum, patient health information that identifies a particular individual with

health- and medical-related information is treated as protectable, although other types of sensitive information in addition to or in lieu of specific patient health information could also be protectable.

5 Preferably, the server 13 is a computing platform configured as a uni-, multi- or distributed processing system, and the clients 19 are general-purpose computing workstations, such as a personal desktop or notebook computer. In addition, the patient management device 12, server 13 and clients 19 are programmable computing devices that respectively execute software programs and include components conventionally found in computing device, such as, for example, a central processing unit (CPU), memory, network interface, persistent storage, and
10 various components for interconnecting these components.

Patient data includes any data that originates from a patient 14 under remote management and can include physiological measures, parametric data, and environmental parameters. The patient data can either be measured or generated directly by an external sensor 17 or can be submitted as already-measured values to a patient management device 12, either directly, such as
15 through a user interface, or indirectly, via, for instance, an external sensor 17 or other device interfaced to the patient management device 12. FIGURE 2 is a process flow diagram showing a method 30 for providing authentication of remotely collected external sensor measures, in accordance with one embodiment. External sensor measures include patient data that have been collected by a source other than an IMD 15 or implantable sensor 16, such as an external sensor
20 17.

By way of example, the collection 31 of patient data 37 can be performed autonomously 34, semi-autonomously 35, and through networked data collection 36. Autonomous patient data collection 34 is performed by an external sensor 17 independently from other devices and includes authentication of the source of the patient data 37, which is forwarded as a complete
25 packet of information. Semi-autonomous data patient collection 35 is performed by an external sensor 17 in conjunction with another device, typically the patient management device 12, which uses the external sensor 17 as a measurement source and records the measurement as patient data 37. Networked data collection 36 is performed by a patient management device 12 or equivalent device, such as a Web-based personal computer, which receives the patient data 37 through a
30 user interface, such as in response to queries presented to the patient 14. Other forms of patient data collection 31 are possible.

The delivery of the patient data 37 to the centralized server 13 and, in a further embodiment, a patient management device 12, is deferred pending the determination 32 of the identification of the source from which the patient data 37 was obtained. In one embodiment,

identification determination 32 is performed passively by relying upon detectable indicia implanted physically into the patient 14, as further described below with reference to FIGURE 3. In a further embodiment, identification determination 32 is performed actively by requiring the patient 14 to submit credentialing information, as further described below with reference to
5 FIGURE 4.

Following successful determination of the source of the patient data 37 as being the patient 14, the patient data 37 can be forwarded 33 for accumulation at the centralized server 13 or other repository to facilitate remote patient management. In further embodiments, the patient data 37 is forwarded on an interim basis to the patient management device 12 or to an IMD 15 or
10 implantable sensor 16 for transient staging, pending eventual forwarding to the centralized server 13. Other forms of patient identification authentication are possible, including incremental or intermediate authentication on a point-to-point basis through passive, active, or combined authentication performed by one or more devices.

Passive authentication relies upon the presence of detectable indicia implanted into the
15 patient 14 to provide the necessary authentication data by which to confirm patient identity. FIGURE 3 is a block diagram showing, by way of example, patient identification through passive authentication 40. By way of example, detectable indicia can include a serial number or other uniquely identifying data internally associated with an IMD or implantable sensor 41, and an implantable identification tag 42, such as a radio frequency identification tag or similar
20 device, which contains uniquely identifying data that can be remotely read. The identifying data is remotely accessed when the patient 14 is within sufficient proximity to ensure that the measurement originated with the patient 14 and not from another source.

The identifying data is compared against stored authentication data that uniquely identifies a specific patient 14. Passive authentication 40 requires the least amount of effort by
25 the patient 14 and relies upon the system 10 to perform authentication transparently to the patient 14. However, the patient 14 must be willing to receive an implantable device, which contains the uniquely identifying data. Other forms of passive authentication are possible.

Active authentication requires the patient 14 to undertake a physical action to provide credentialing information by which to confirm patient identity. FIGURE 4 is a block diagram
30 showing, by way of example, patient identification through active authentication 50. By way of example, active authentication 50 can utilize biometric identifiers 51, token identifiers 52, and code entry identifiers 53. Biometric identifiers 51 use a physical property of the patient 14, such as retina or iris pattern, fingerprint, voice pattern, personal identification number, or identification token, to uniquely identify the patient 14. However, biometric identifiers 51 may

not be suitable for all patients 14, such as the infirm, elderly, or physically challenged. In a further embodiment, a token identifier 52, such as an identification card containing credentialing information, must be presented by the patient 14 prior to the system 10 accepting patient data for forwarding. Token identifiers 52, though, are susceptible to compromise, should the physical
5 token be used by another person. In a still further embodiment, code entry identifier 53 assigns a personal identification number (PIN) or similar code to uniquely identify the patient 14. Code entry identifiers 53 are also susceptible to compromise, but can remain secure, as long as the patient 14 keeps the code identifier confidential. Other forms of active authentication are possible.

10 Autonomous patient data collection 34 (shown in FIGURE 2) requires an external sensor to incorporate the capability of authenticating a patient. FIGURE 5 is a functional block diagram showing patient identification 60 with an external sensor 61. The capability to authenticate a patient 14 is provided by supplementing the external sensor 61 with an input device 63, which
15 can perform one or more forms of active patient identification, such as receiving a retina or iris pattern, fingerprint, voice pattern, personal identification number, or identification token. The external sensor 61 also stores authentication data 62 that is maintained in a form suitable for automated comparison to the results of the input device 63. Suitable input devices include a retinal or iris scanner, fingerprint scanner, voice input device, keypad, barcode scanner, or magnetic card reader. Other forms of input devices for active patient identification and for
20 storing correspondingly suitable authentication data are possible.

Autonomous patient data collection 34 is performed by the external sensor 61 independent from the centralized server, patient management device, and other devices. The external sensor 61 defers forwarding the collected patient data to the patient management device 12 or, in a further embodiment, the centralized server 13, pending confirmation of patient
25 identity. FIGURE 6 is a flow diagram showing patient identification 70 with an external sensor 61. Initially, a measurement is measured or accepted by the external sensor 61 (block 71). The measurement can be displayed, but will not be forwarded from the external sensor 61, pending authentication of the identity of the source from which the measurement was collected. Identifying data is solicited and obtained from the user (block 72), such as by prompt or
30 displayed message. Identifying data provided by the user is accepted and compared to the authentication data 62 (block 73). If the identifying data matches the authentication data 62 (block 74), the measurement is forwarded (block 75) to the patient management device 12 or, in a further embodiment, the centralized server 13. Otherwise, the measurement is rejected (block 76).

Patient management devices must also include the capability to confirm patient identification when performing semi-autonomous patient data collection 35 or networked data collection 36. FIGURE 7 is a functional block diagram showing patient identification 80 with a patient management device 81. The capability to authenticate a patient 14 is provided by supplementing the patient management device 81 with an input device 83, which can perform one or more forms of active patient identification, such as receiving a retina or iris pattern, fingerprint, voice pattern, personal identification number, or identification token. The patient management device 81 also stores authentication data 82 that is maintained in a form suitable for automated comparison to the results of the input device 83. Suitable input devices include a retinal or iris scanner, fingerprint scanner, voice input device, keypad, barcode scanner, or magnetic card reader. Other forms of input devices for active patient identification and for storing correspondingly suitable authentication data are possible.

Similar to the autonomous patient data collection 34 performed by an external sensor 61, each patient management device 81 defers forwarding the collected patient data to the centralized server 13 pending confirmation of patient identity. FIGURE 8 is a flow diagram showing patient identification 90 with a patient management device. Initially, a measurement is measured or accepted by an external sensor 17 (block 91) and is received or accepted at the patient management device 81 (block 92). The measurement can be displayed, but the measurement will not be forwarded from the patient management device 81, pending authentication of the identity of a source from which the measurement was collected. Identifying data is solicited and obtained from the user (block 93), such as by prompt or displayed message. Identifying data provided by the user is accepted and compared to the authentication data 82 (block 94). If the identifying data matches the authentication data 82 (block 95), the measurement is forwarded (block 96) to the centralized server 13. Otherwise, the measurement is rejected (block 97).

Passive authentication requires detectable indicia generally available through a device implanted in the patient 14, such as an IMD, implantable sensor, or implantable identification tag. FIGURES 9, 11, and 13 are functional block diagrams showing patient identification 100, 120, 140 with an implantable medical device 103, 123, 143. A separate input device is not required, as the implantable medical device itself serves as the device by which patient identity is confirmed. FIGURES 10, 12, and 14 are flow diagrams showing patient identification 110, 130, 150 with an implantable medical device 103, 123, 143. The implantable device containing the detectable indicia is referred to generally as an implantable medical device, but also includes

implantable sensors, implantable identification tags, and other forms of implantable devices that can be uniquely associated with a patient 14 through remote detection.

Prior to being forwarded to the centralized server 13, the patient data can be transiently staged at either an external sensor, patient management device, or implantable medical device.

5 Transiently staging patient data at a patient management device enables the patient data to be forwarded to the centralized server immediately upon authentication, but consumes storage on the patient management device if the authentication fails and the patient data must ultimately be discarded as spurious. Referring to FIGURE 9, a patient management device 102 that is in receipt of patient data 104 received or accepted from an external sensor 101 confirms the
10 presence of an implantable medical device 103. The patient management device 102 utilizes near field telemetry, such as induction, or far field telemetry, such as radio frequency communication, to attempt to communicate with the implantable medical device 103. A failure of communication implies that the implantable medical device 103 and, therefore, the patient 14 are not present and the patient data 104 is discarded as spurious.

15 Referring next to FIGURE 10, initially, a measurement is measured or accepted by the external sensor 101 (block 111) and is received or accepted by the patient management device 102 (block 112). Upon receiving the measurement, the patient management device 102 attempts to communicate with the implantable medical device 103 (block 113). If the communication attempt is successful (block 114), the measurement is forwarded by the patient management
20 device 102 as patient data 104 to the centralized server 13 (block 115). Otherwise, the measurement is rejected as spurious (block 116).

Transiently staging the patient data on an external sensor avoids consuming storage on a patient management device if authentication fails, but can incur a delay in forwarding the patient data to the centralized server while the patient data is forwarded from the external sensor to the
25 patient management device. Referring next to FIGURE 11, an external sensor 121 that has measured or accepted patient data 124 confirms the presence of an implantable medical device 123. The external sensor 121 utilizes near field telemetry, such as induction, or far field telemetry, such as radio frequency communication, to attempt to communicate with the implantable medical device 123. A failure of communication implies that the implantable
30 medical device 123 and, therefore, the patient 14 are not present and the patient data 124 is discarded as spurious. Discarded patient data is never actually received by the patient management device 122.

Referring next to FIGURE 12, initially, a measurement is measured or accepted by the external sensor 121 (block 131). The external sensor 121 attempts to communicate with the

implantable medical device 123 (block 132). If the communication attempt is successful (block 133), the measurement is received or accepted by the patient management device 122 (block 134) and is forwarded to the centralized server 13 (block 135). Otherwise, the measurement is rejected as spurious (block 136).

5 Transiently staging the patient data on an implantable medical device avoids involving a patient management device in authentication, but is expensive in terms of the resources consumed, as the implantable medical device must expend processing, storage, and power budget resources to temporarily hold the patient data pending forwarding to the patient management device. The implantable medical device must have sufficient resources to
10 temporarily hold the patient data pending upload to the patient medical device. Referring next to FIGURE 13, an external sensor 141 sends patient data 144 to an implantable medical device 143 that is implanted in the patient 14. To guard against patient data being uploaded to the implantable medical device 143 that originated from a source other than the patient 14, the external sensor 141 and implantable medical device 143 must be in close physical proximity so
15 as to ensure that the patient data source is the patient with the implantable medical device 143. The requirement for close physical proximity implicitly provides patient identification authentication and, accordingly, the patient data 143 can be forwarded to the patient management device 142 at the next interrogation for eventual forwarding to the centralized server 13.

Referring next to FIGURE 14, the external sensor 141, patient management device 142,
20 and implantable medical device 143 each participate, but only the implantable medical device 143 directly interfaces to both the external sensor 141 and patient management device 142. Initially, a measurement is measured or accepted by the external sensor 141 (block 151), which then attempts to communicate with the implantable medical device 143 (block 152). In one embodiment, the external sensor 141 uses near field telemetry, such as induction, to ensure close
25 physical proximity of the patient 14. In a further embodiment, the external sensor 141 uses far field telemetry, such as radio frequency communication, that is set to a short transmission range to ensure close physical proximity of the patient 14. If the communication attempt is successful (block 153), the measurement is forwarded to the implantable medical device 143 (block 154) and is eventually provided to the patient management device 142 at the next data interrogation
30 (block 156) for eventual forwarding to the centralized server 13. Otherwise, the measurement is implicitly rejected as spurious through non-delivery to the implantable medical device 143 (block 155).

In one embodiment, a single patient data source can be associated with a specific patient in a one-to-one mapping, which provides local authentication. In a further embodiment, a single

patient data source can be associated with multiple patients in a one-to-many mapping.

FIGURES 15 and 16 are functional block diagrams showing patient identification 160, 170 for multiple patients, in accordance with one embodiment. One-to-many mappings can be used, for example, to enable multiple patients to share a single external medical sensor 17 or, where
5 appropriate, external medical devices, or to provide data from an implantable or external medical sensor or device, subject to proper credentialing. Referring first to FIGURE 15, patient identification 160 through local authentication can be provided by maintaining multiple sets of patient credentials 165 at a patient data source 161. Each patient credentials set 165 is associated with a specific patient 164 and the patient data source 161 accepts readings of physiological
10 measures only from those users authorized through the maintained patient credentials sets 165. Authenticated patient data 166 is forwarded to a centralized server 163 through an internetwork 162, which can include one or more intermediate patient management devices (not shown).

Referring next to FIGURE 16, patient identification 170 through remote authentication can be provided by accepting a set of credentials 175 associated with a particular patient 174 at a
15 patient data source 171. The patient data source 171 or, in a further embodiment, a patient management device (not shown), will reject patient data collected or read from users that fail to provide authenticating patient credentials sets. Otherwise, physiological data and the patient credentials set 176 are forwarded to a centralized server 173 over an internetwork 172, which can include one or more intermediate patient management devices (not shown), for authentication by
20 a centralized server 173. The centralized server 173 will authenticate patient data collected or read from authorized users and will reject patient data collected or read from unauthorized users. Other one-to-many, as well as many-to-many, mappings are possible.

While the invention has been particularly shown and described as referenced to the embodiments thereof, those skilled in the art will understand that the foregoing and other
25 changes in form and detail may be made therein without departing from the spirit and scope of the invention.

CLAIMS:

1 1. A system (10) for providing authentication of remotely
2 collected external sensor (17) measures, comprising:
3 a collection module (17) to collect (31) physiological measures (37)
4 from a source situated remotely from a repository for accumulating such
5 collected physiological measures (37);
6 an identification module (12) to determine an identification (32) of the
7 source from which the physiological measures (37) were collected (31) against
8 authentication data (82) that uniquely identifies a specific patient (14); and
9 a staging module (15) to forward (33) the physiological measures (37)
10 to the repository upon authenticating the patient identification (80) as
11 originating from the specific patient (14).

1 2. A system (10) according to Claim 1, wherein the collection
2 module (17) comprises at least one of a discrete external sensor (17), an
3 external sensor (17) operatively coupled to a patient management device (12),
4 and a patient management device (12) passively receiving the physiological
5 measures (37).

1 3. A system (10) according to Claim 2, wherein the external
2 sensor (17) comprises at least one of a weight scale, blood pressure cuff,
3 glucometer, thermometer, and spirometer.

1 4. A system (10) according to Claim 1, wherein the patient
2 identification (80) is passively determined (40) through use of at least one of
3 an implantable medical device (15) and radio frequency identification tag (42),
4 which each comprise authentication data (82).

1 5. A system (10) according to Claim 1, wherein the patient
2 identification (80) is actively determined (50) through use of at least one of a
3 biometric identifier (51), token identifier (52), and code entry identifier (53),
4 which each provide credentials for comparison to the authentication data (82).

- 1 6. A system (10) according to Claim 1, wherein the staging
2 module (15) comprise at least one of an external sensor (17), patient
3 management device (12), and implantable medical device (15).
- 1 7. A system (10) according to Claim 1, further comprising:
2 an external sensor (17) on which to implement the authentication data
3 (82);
4 a store to hold the physiological measures (37) on the external sensor
5 (17) until the patient identification (80) is confirmed, wherein the
6 physiological measures (37) are provided to a patient management device (12)
7 upon confirmation.
- 1 8. A system (10) according to Claim 1, further comprising:
2 a patient management device (12) on which to implement the
3 authentication data (82);
4 an external sensor (17) to provide the physiological measures (37) to
5 the patient management device (12); and
6 a store to hold the physiological measures (37) on the patient
7 management device (12) until the patient identification (80) is confirmed.
- 1 9. A system (10) according to Claim 1, further comprising:
2 an external sensor (17) to provide the physiological measures (37) to a
3 patient management device (12);
4 a communications module to confirm proximity of an implantable
5 medical device (15) to the patient management device (12); and
6 a store to hold the physiological measures (37) on the patient
7 management device (12) until the implantable medical device (15) proximity
8 is confirmed.
- 1 10. A system (10) according to Claim 1, further comprising:
2 a communications module to confirm communication between an
3 implantable medical device (15) and an external sensor (17), wherein the
4 physiological measures (37) are provided to a patient management device (12)
5 upon confirmation.

1 11. A system (10) according to Claim 1, further comprising:
2 a communications module to confirm communication between an
3 implantable medical device (15) and an external sensor (17), wherein the
4 physiological measures (37) are provided to the implantable medical device
5 (15) upon confirmation.

1 12. A system (10) according to Claim 1, further comprising:
2 patient data (37) included with the forwarded (33) physiological
3 measures (37) comprising at least one of psychological, drug dosing, medical
4 therapy, insurance-related, digital imagery or sound, and patient-provided or
5 -uploaded information.

1 13. A method (30) for providing authentication of remotely
2 collected external sensor (17) measures, comprising:
3 collecting (31) physiological measures (37) from a source situated
4 remotely from a repository for accumulating such collected physiological
5 measures (37);
6 determining an identification (32) of the source from which the
7 physiological measures (37) were collected (31) against authentication data
8 (82) that uniquely identifies a specific patient (14); and
9 forwarding (33) the physiological measures (37) to the repository upon
10 authenticating the patient identification (80) as originating from the specific
11 patient (14).

1 14. A method (30) according to Claim 13, further comprising:
2 collecting (31) the physiological measures (37) using at least one of a
3 discrete external sensor (17), an external sensor (17) operatively coupled to a
4 patient management device (12), and a patient management device (12)
5 passively receiving the physiological measures (37).

1 15. A method (30) according to Claim 14, wherein the external
2 sensor (17) comprises at least one of a weight scale, blood pressure cuff,
3 glucometer, thermometer, and spirometer.

1 16. A method (30) according to Claim 13, further comprising:

2 passively determining (40) the patient identification (80) through use
3 of at least one of an implantable medical device (15) and radio frequency
4 identification tag (42), which each comprise authentication data (82).

1 17. A method (30) according to Claim 13, further comprising:
2 actively determining (50) the patient identification (80) through use of
3 at least one of a biometric identifier (51), token identifier (52), and code entry
4 identifier (53), which each provide credentials for comparison to the
5 authentication data (82).

1 18. A method (30) according to Claim 13, further comprising:
2 forwarding (33) the physiological measures (37) from at least one of an
3 external sensor (17), patient management device (12), and implantable
4 medical device (15).

1 19. A method (30) according to Claim 13, further comprising:
2 implementing the authentication data (82) on an external sensor (17);
3 holding the physiological measures (37) on the external sensor (17)
4 until the patient identification (80) is confirmed; and
5 providing the physiological measures (37) to a patient management
6 device (12) upon confirmation.

1 20. A method (30) according to Claim 13, further comprising:
2 implementing the authentication data (82) on a patient management
3 device (12);
4 providing the physiological measures (37) to the patient management
5 device (12) from an external sensor (17); and
6 holding the physiological measures (37) on the patient management
7 device (12) until the patient identification (80) is confirmed.

1 21. A method (30) according to Claim 13, further comprising:
2 providing the physiological measures (37) to a patient management
3 device (12) from an external sensor (17);
4 confirming proximity of an implantable medical device (15) to the
5 patient management device (12); and

6 holding the physiological measures (37) on the patient management
7 device (12) until the implantable medical device (15) proximity is confirmed.

1 22. A method (30) according to Claim 13, further comprising:
2 confirming communication between an implantable medical device
3 (15) and an external sensor (17); and
4 providing the physiological measures (37) to a patient management
5 device (12) upon confirmation.

1 23. A method (30) according to Claim 13, further comprising:
2 confirming communication between an implantable medical device
3 (15) and an external sensor (17); and
4 providing the physiological measures (37) to the implantable medical
5 device (15) upon confirmation.

1 24. A method (30) according to Claim 13, further comprising:
2 including patient data (37) with the forwarded (33) physiological
3 measures (37) comprising at least one of psychological, drug dosing, medical
4 therapy, insurance-related, digital imagery or sound, and patient-provided or
5 -uploaded information.

1 25. A computer-readable storage medium holding code for
2 performing the method (30) according to Claim 13.

1 26. An apparatus for providing authentication of remotely collected
2 external sensor (17) measures, comprising:
3 means for collecting (31) physiological measures (37) from a source
4 situated remotely from a repository for accumulating such collected
5 physiological measures (37);
6 means for determining an identification (32) of the source from which
7 the physiological measures (37) were collected (31) against authentication
8 data (82) that uniquely identifies a specific patient (14); and
9 means for forwarding (33) the physiological measures (37) to the
10 repository upon authenticating the patient identification (80) as originating
11 from the specific patient (14).

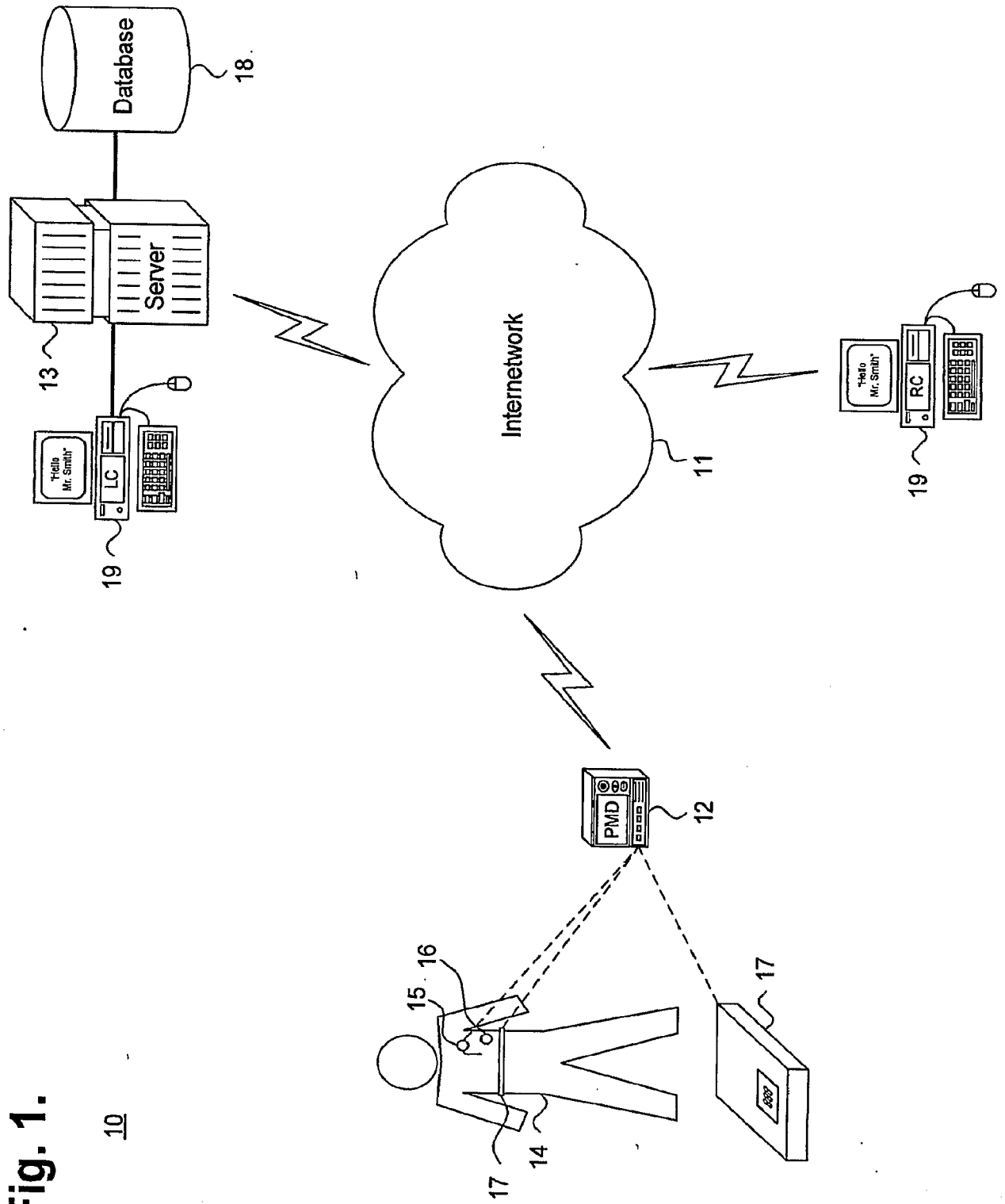


Fig. 1.

Fig. 2.

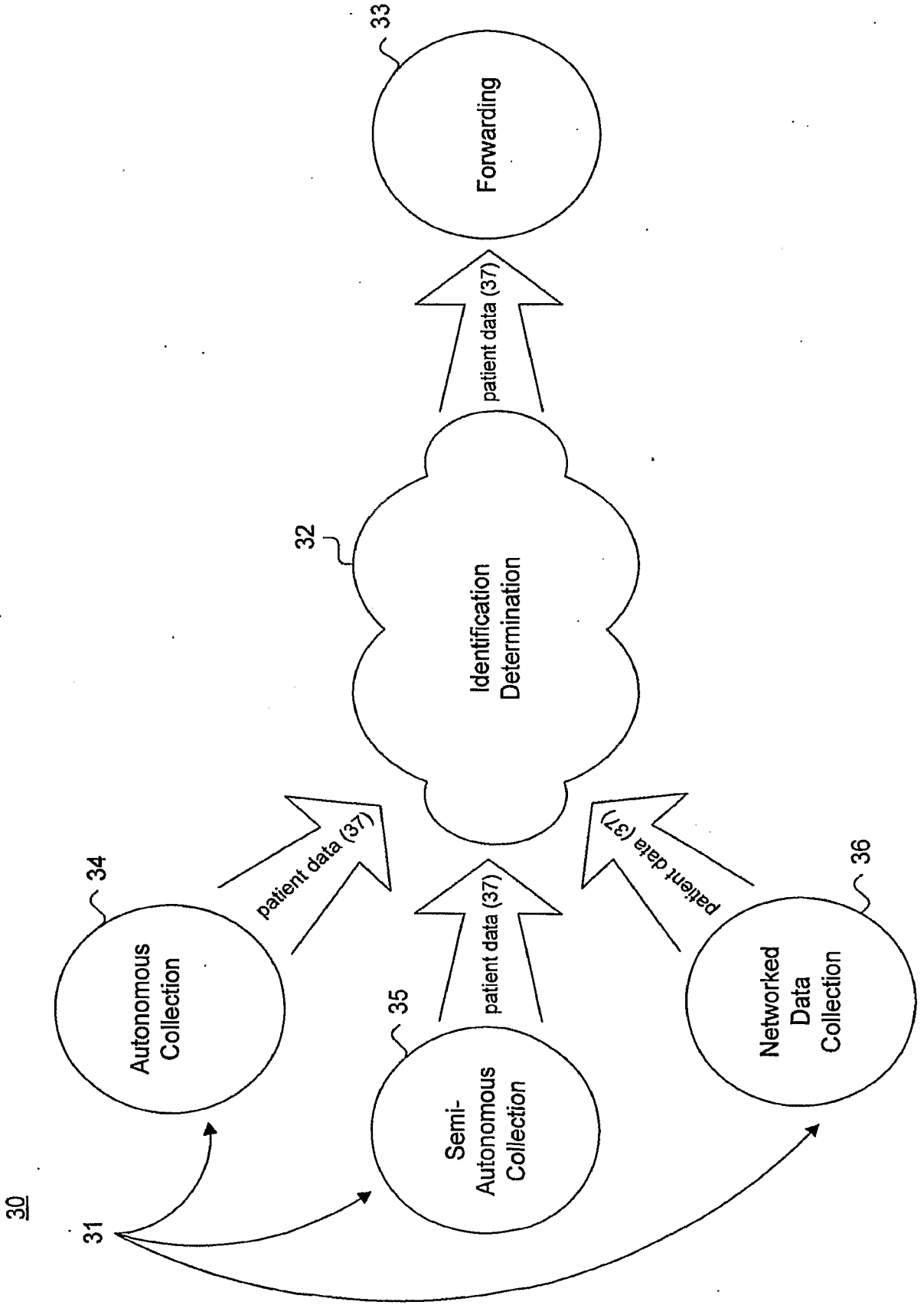


Fig. 3.

40

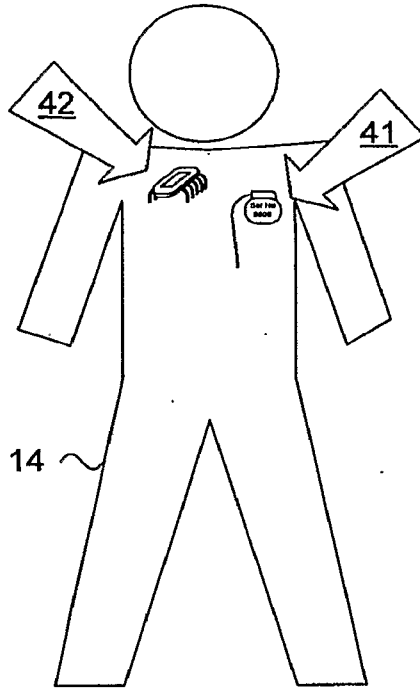


Fig. 4.

50

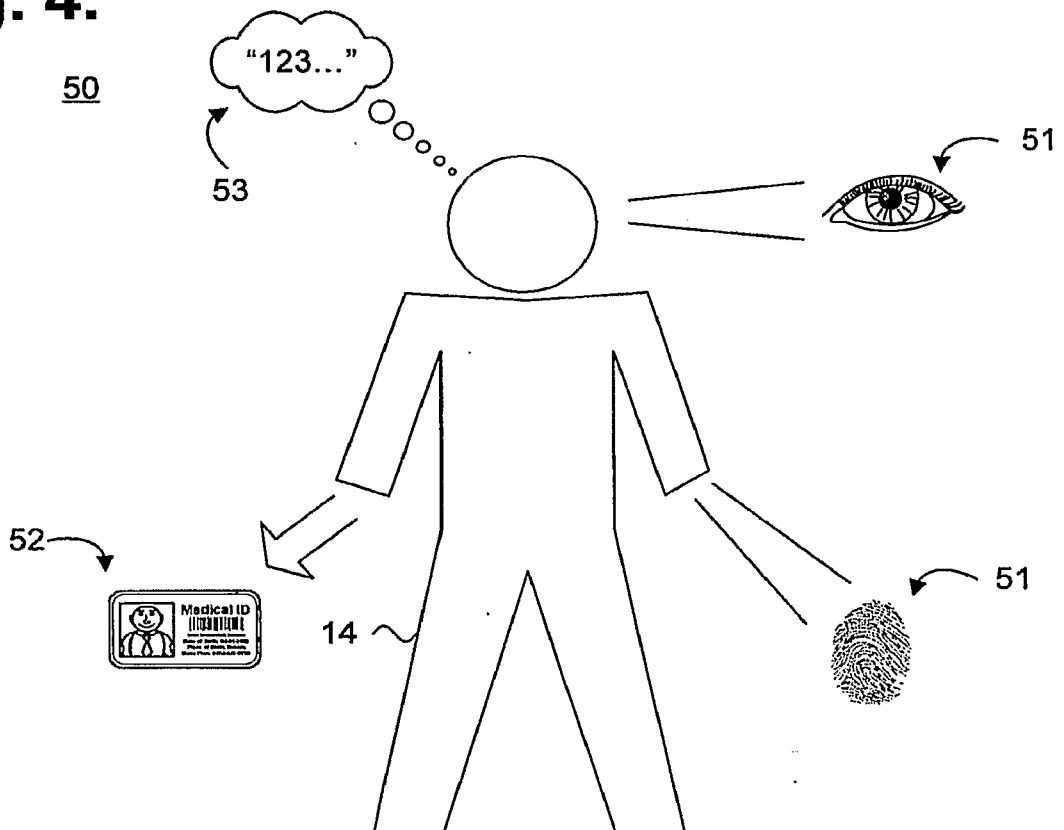


Fig. 5.

60

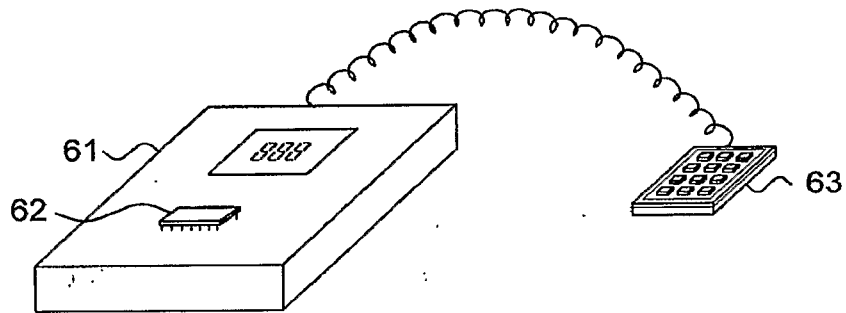


Fig. 6.

70

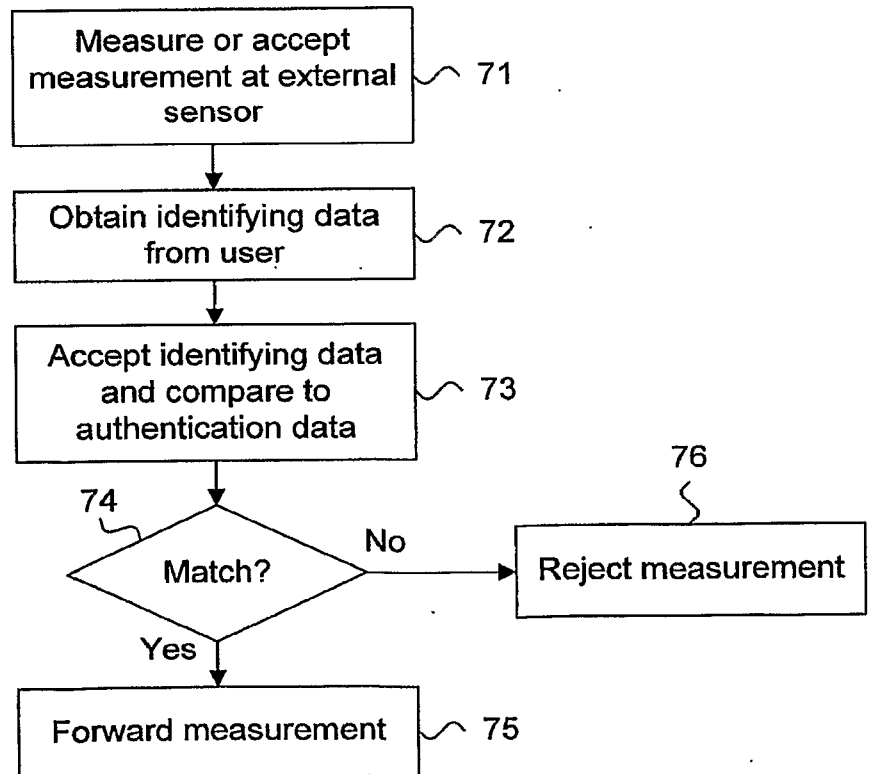


Fig. 7.

80

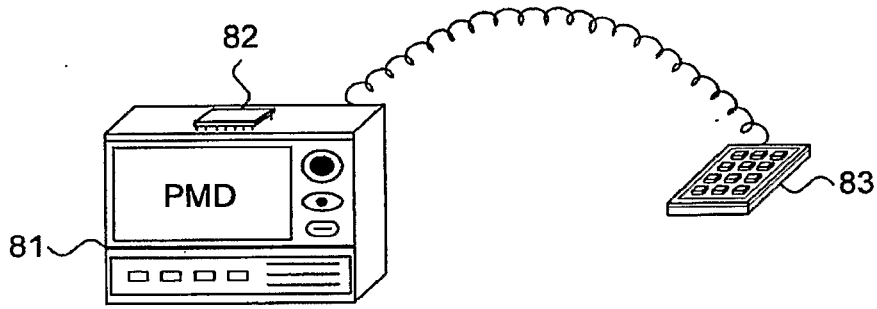


Fig. 8.

90

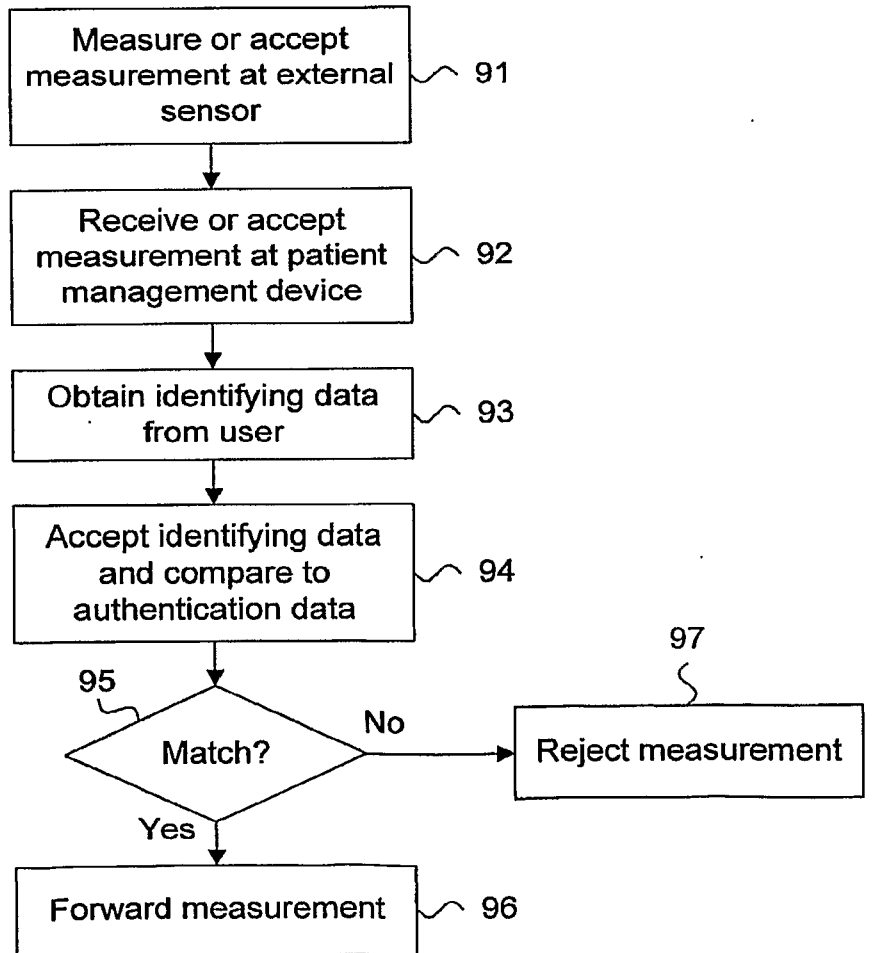


Fig. 9.

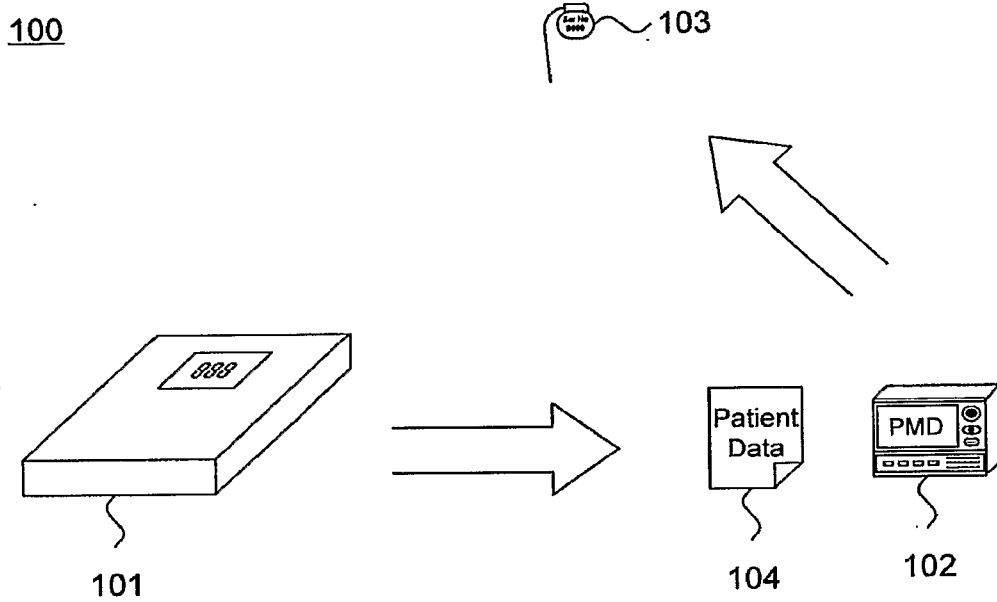


Fig. 10.

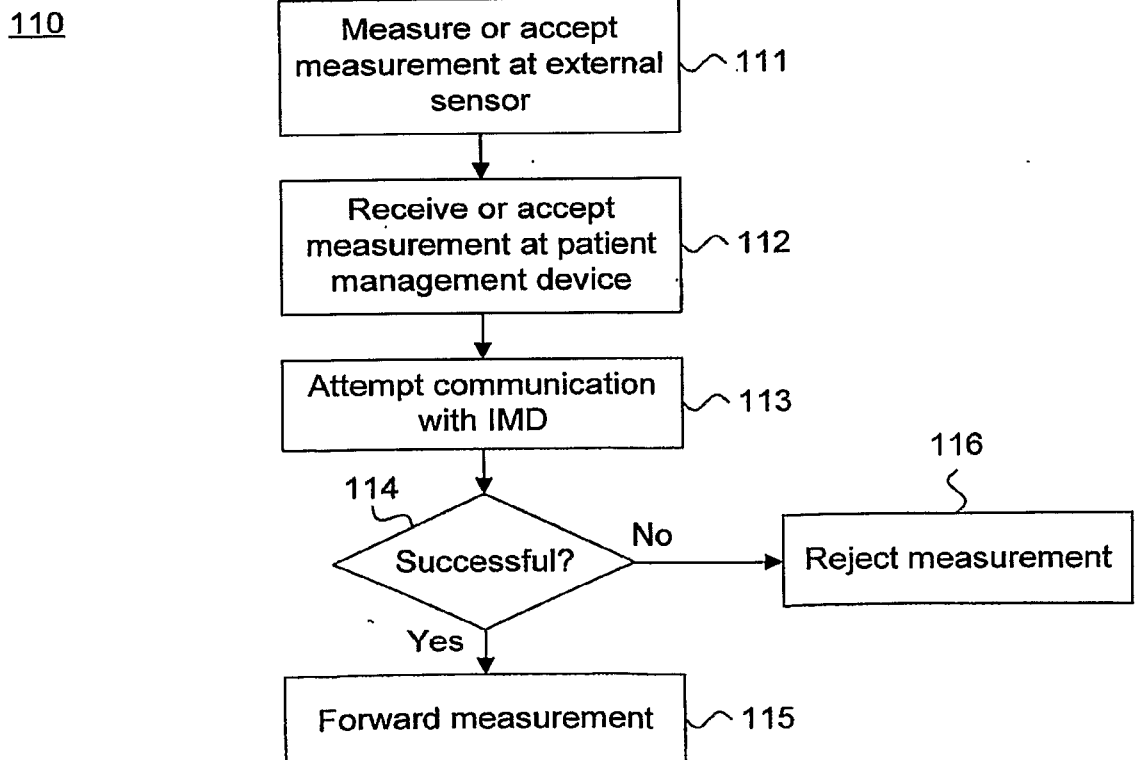


Fig. 11.

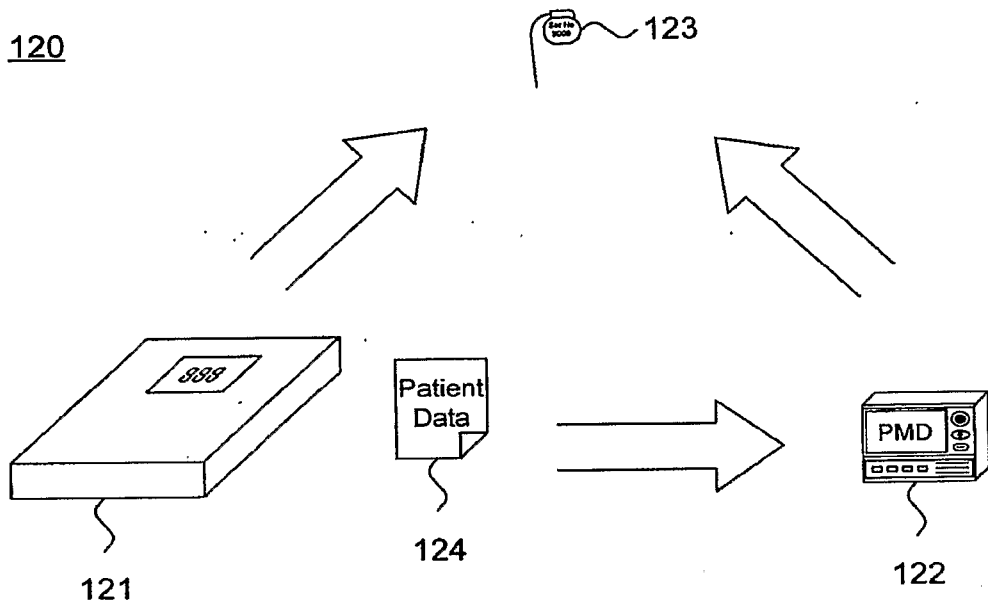


Fig. 12.

130

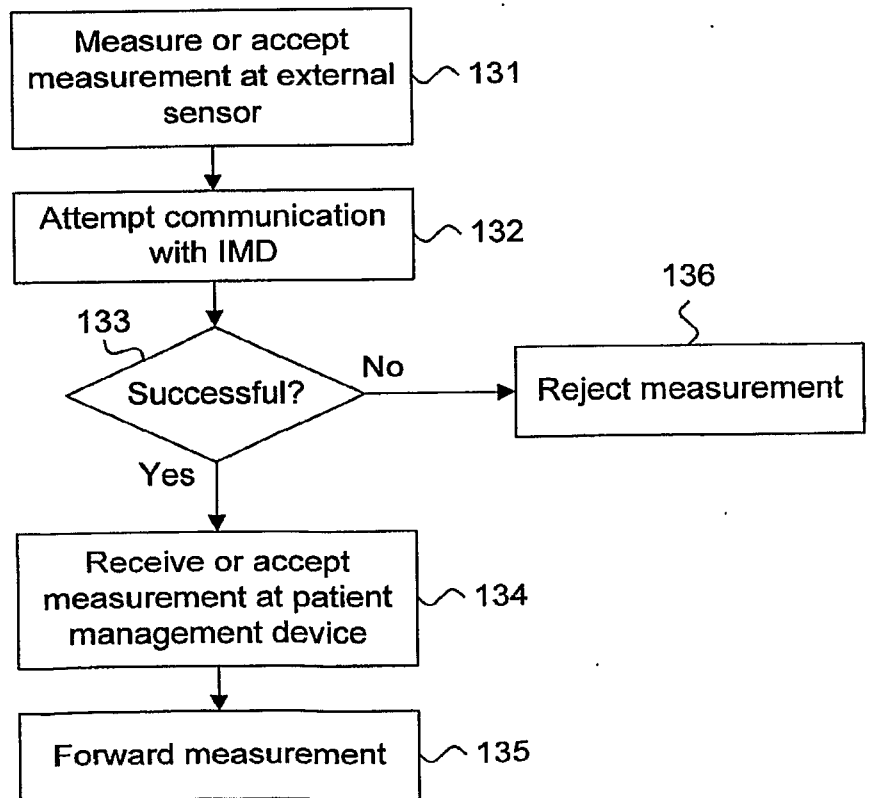


Fig. 13.

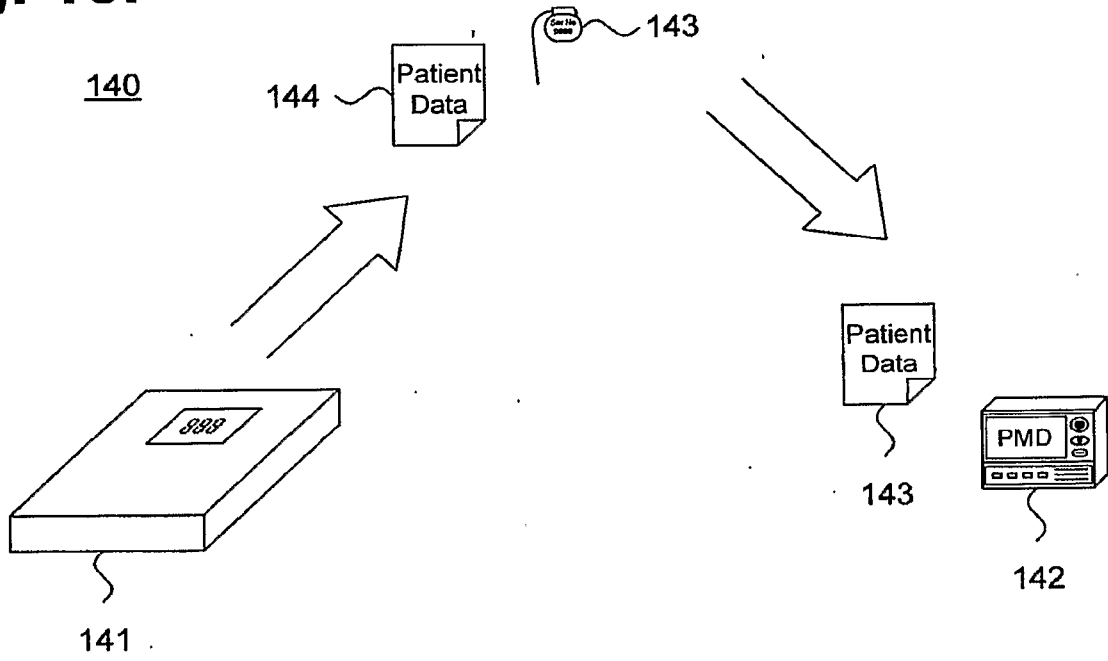
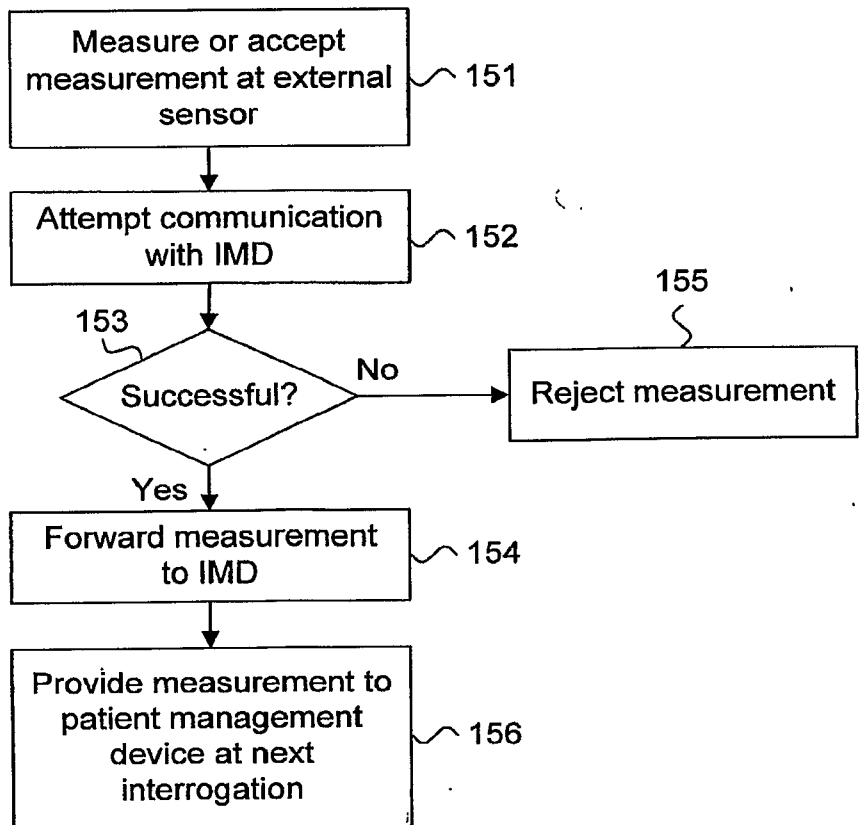


Fig. 14.

150



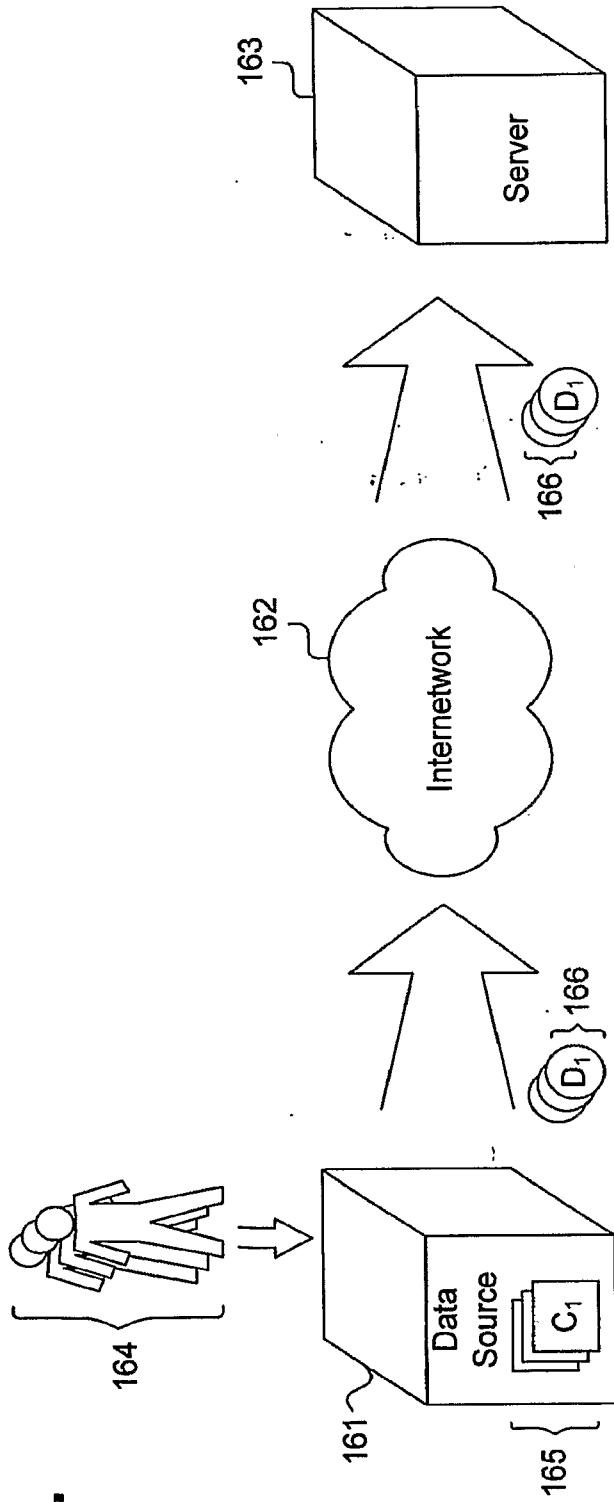


Fig. 15.

160

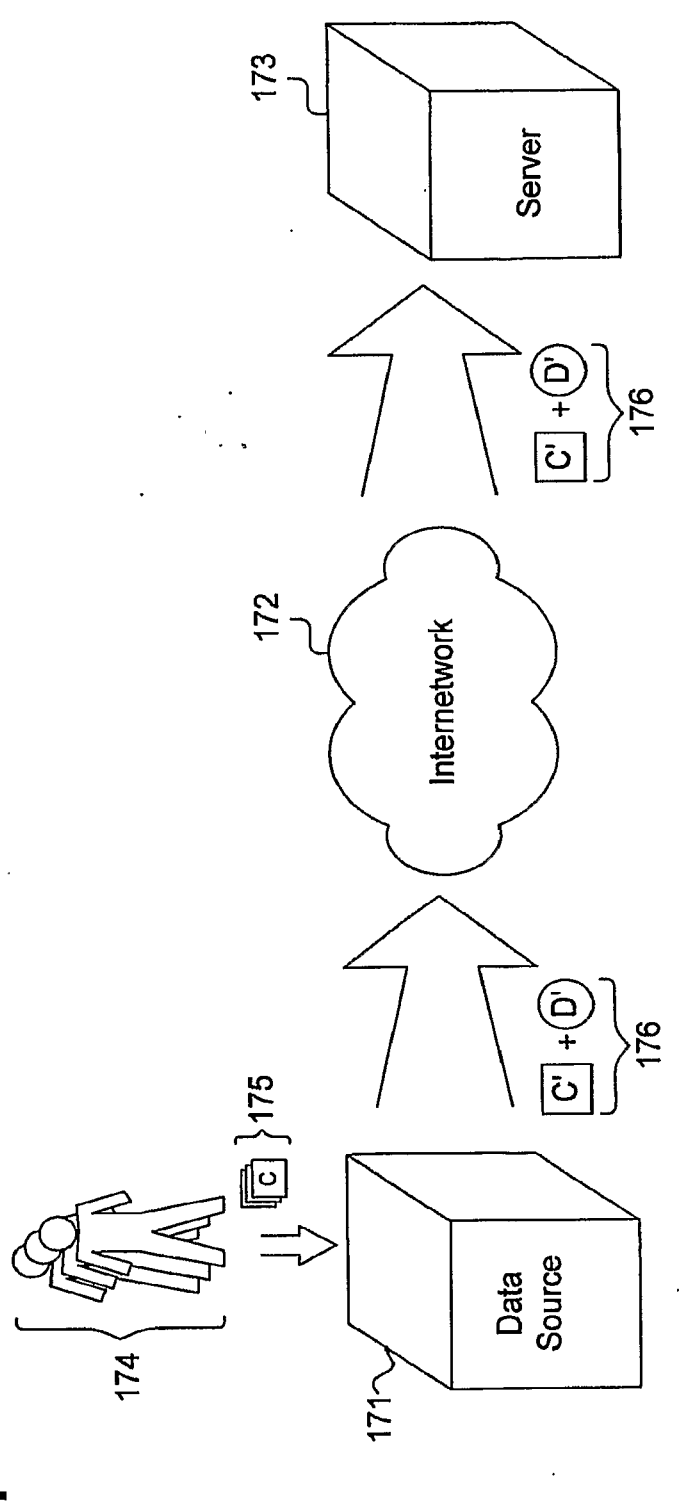


Fig. 16.

170

专利名称(译)	提供远程收集的外部传感器测量的认证		
公开(公告)号	EP1959820A2	公开(公告)日	2008-08-27
申请号	EP2006845324	申请日	2006-12-11
[标]申请(专利权)人(译)	心脏起搏器股份公司		
申请(专利权)人(译)	心脏起搏器, INC.		
当前申请(专利权)人(译)	心脏起搏器, INC.		
[标]发明人	DONG YANTING CARPENTER TODD P NI QUAN HOYME KENNETH P		
发明人	DONG, YANTING CARPENTER, TODD P. NI, QUAN HOYME, KENNETH P.		
IPC分类号	A61B5/00		
CPC分类号	A61B5/0002 A61B5/117 G06F19/3418 G06Q50/24 G16H40/67 A61B5/1171		
优先权	11/301214 2005-12-12 US		
外部链接	Espacenet		

摘要(译)

提出了一种用于提供远程收集的外部传感器 (17) 测量的认证的系统 (10) 和方法 (30)。从位于远离储存库 (18) 的源 (17) 收集 (31) 生理措施 (37)，用于累积这种收集的生理措施 (37)。根据唯一识别特定患者 (14) 的认证数据 (82) 确定从其收集生理测量 (37) 的源的标识 (32) (31)。在将患者标识 (80) 认证为源自特定患者 (14) 时，将生理测量 (37) 转发 (33) 到存储库。