REMOTE MONITORING SYSTEMS AND METHODS FOR MEDICAL DEVICES

FIELD

[001] The present application is directed to a remote monitoring system for monitoring medical devices in communication with a wireless communication network, and more particularly, to a remote monitoring system having a plurality of monitoring devices for monitoring medical devices that communicate with the wireless communication network via one or more wireless relay modules and a wireless relay network.

BACKGROUND

[002] In critical care and home care health service centers, including hospitals, clinics, assisted living centers and the like, care giver-patient interaction time is at a premium. Moreover, response times by care givers to significant health conditions and events can be critical. Systems of centralized monitoring have been developed to better manage care giver time and patient interaction. In such systems, physiological data from each patient is transmitted to a centralized location. At this centralized location, a single or small number of technicians monitor all of this patient information to determine patient status. Information indicating a patient alarm condition will cause the technicians and/or system to communicate with local care givers to provide immediate patient attention, for example via wireless pagers and/or cell phones, and/or by making a facility-wide audio page.

[003] Implementing such centralized monitoring systems using wireless networks may present a number of difficulties. In order to effectively monitor patient status using information provided by a variety of medical devices that may be dynamically assigned to patients in a variety of rooms and on a variety of floors in a facility, it would be desirable to establish communications between the medical devices and the centralized location by means of a local area network such as, for example, a "WiFi" network based on IEEE 802.11 standards. However, as such networks are typically already in place in facilities to support a variety of other functions (for example, physician access to electronic medical

records (EMRs), facility administrative systems and other functions), it is often undesirable to secure sufficient local area network access for the purpose of providing centralized monitoring. Moreover, when a patient is located remotely from a critical care health service center (for example, at home), access to traditional local area network facilities such as a WiFi network may be unavailable or not sufficiently reliable to support critical care monitoring applications.

[004] For improved efficiencies in centralized monitoring of critical care and home care health service centers, it may be desirable to provide a single "off-site" centralized monitoring location for monitoring several geographically-dispersed critical care health service centers.

[005] As an alternative to conventional WiFi or IEEE 801.11-based local area networks, ZIGBEE networks based on the IEEE 802.15.4 standard for wireless personal area networks have been used for collecting information from a variety of medical devices in accordance with IEEE 11073 Device Specializations for point-of-care medical device communication, including for example pulse oximeters, blood pressure monitors, pulse monitors, weight scales and glucose meters. See, e.g., *ZIGBEE Wireless Sensor Applications for Health, Wellness and Fitness*, the ZIGBEE Alliance, March 2009, which is incorporated by reference herein in its entirety. As compared to present IEEE 802.15.1 Bluetooth wireless personal area networks, for example, ZIGBEE networks provide the advantage of being dynamically configurable, for example, in "self-healing" mesh configurations, and operating with low power requirements (enabling, for example, ZIGBEE transceivers to be integrally coupled to the medical devices under battery power). However, transmission ranges between individual ZIGBEE transceivers are generally limited to no more than several hundred feet. As a consequence, such networks are suitable for on-site communications with medical devices, but unusable for centralized monitoring locations located off-site.

[006] Therefore, a hybrid system may be employed in which one or more wireless personal area networks are configured to facilitate on-site communications between medical devices and one or more wireless relay modules which are further configured to communicate with off-site centralized monitoring systems (for example, via a wireless wide-area network (WWAN) such as a mobile telephone data network, for example, based on a Global System for Mobile Communications (GSM) or Code Division

Multiple Access (CDMA) cellular network or associated wireless data channels). Such a relay module and system are respectively described in the related patent applications entitled "Wireless Relay Module for Remote Monitoring Systems," U.S. Application Ser. No. 13/006,769 , filed January 14, 2011 and "Medical Device Wireless Network Architectures," U.S. Application Ser. No. 13/006,784 , filed January 14, 2011) which have been incorporated by reference herein for all purposes.

[007] In accordance with applicable patient data privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), communication of information between the monitored medical devices and the central monitoring location must be done securely, and medical device and associated patient information must be made available only to personnel accessing the centralized monitoring systems who are in possession of the appropriate access credentials. In order to be viable, the centralized monitoring system must also be capable of recognizing medical device information indicating an alert condition requiring response by on-site or other specialized personnel and reaching those on-site or specialized personnel to report the alert condition in a timely fashion.

[008] Thus, it would be desirable to provide a remote, centralized medical information monitoring system that communicates over a wireless network of wide reach (for example, a wireless wide area network) with one or more critical care and/or home care health service centers via one or more wireless relay modules at each site, where the wireless relay modules relay communications provided by on-site medical devices over a wireless local area network or wireless personal area network. It would further be desirable for the centralized medical information monitoring system to be capable of also configuring medical devices according to associations with individual sites and patients, of logging communications from medical devices, of displaying medical device data to users of the centralized medical information monitoring system who are able to provide sufficient credentials, and of recognizing medical device alert conditions and reporting these conditions to responsible personnel in a timely fashion.

SUMMARY

[009] The present invention is directed to a remote monitoring system and method for monitoring the status of a plurality of medical devices located remotely from the monitoring system at a patient care or home care facility. In accordance with one embodiment of the invention, one or more medical devices (including but not limited to respirators, enteral feeding devices, pulse oximeters, blood pressure monitors, pulse monitors, weight scales and glucose meters) are provided at a patient care or home care facility. An interface circuit is coupled to each medical device, and is configured for communicating with one of a plurality of the wireless relay modules via a wireless relay network. The wireless relay modules are further configured to communicate with the remote monitoring device over an internet-accessible wireless communication network, and preferably, a wireless wide-area network (WWAN) such as a mobile telephone data network including (for example, based on a Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA) cellular network or associated wireless data channels). Also, for compliance for example with HIPAA regulations, communications over each of the wireless networks are preferably conducted securely.

[0010] The remote monitoring system and method includes a device integration server in communication with the wireless relay modules for receiving data packets from the wireless relay modules including information provided by the medical devices. This information includes identification of an associated medical device and may include data of the medical device, and is preferably encrypted or otherwise securely transmitted, for example, in compliance with HIPAA patient data privacy provisions. In addition, the information may include encrypted or otherwise securely transmitted patient identification information, which in addition may preferably be coded in its unencrypted state to avoid any reference to the patient's identity.

[0011] The remote monitoring system also includes a data management system including a secure device web server and a device control database, and an outbound web server. The data management system is configured to log information provided to the device integration server concerning the medical devices. The outbound web server (alternatively referred to as "web server" herein) is configured to provide webpages including the data of the medical devices for display on a first and second remote

monitoring devices, subject to authentication of an associated data request originating from the monitoring device. The second monitoring device may advantageously be for use by a relative of the patient, such as a parent, caregiver or nurse, who may be located proximate or remote to the patient.

[0012] In accordance with a further aspect of the concepts described herein, a system for enabling the remote monitoring of at least one medical device includes a device integrator server in communication with at least one wireless relay device configured to transmit data packets containing information provided by at least one medical device. Each data packet includes medical device data and at least a medical device identifier or a patient identifier. The system further includes a web server separate from the device integrator server. The web server is configured to provide web pages and to receive at least the medical data.

[0013] In one embodiment the web server is coupled to a first remote monitoring device via a secure internet connection and is configured to receive medical device data and transmit the medical device data to the first remote monitoring device. In one embodiment, the first remote monitoring device displays the medical device data.

[0014] In one embodiment, the web server further transmits at least a portion of the medical device data to a second remote monitoring device for displaying the portion of the medical device data at the second remote monitoring device.

[0015] In one embodiment, the system further includes a data manager system coupled to the device integrator server. The data manager system includes at least a device control database.

[0016] In one embodiment, the web server is configured to verify the patient identifier and medical device identifier before transmitting the medical device data to the first remote monitoring device over the secure internet connection.

[0017] In one embodiment, the web server is configured to transmit the portion of the medical device data to the second remote monitoring device over a path which includes a wireless data link.

[0018] In one embodiment, the wireless data link is over a wireless mobile data network.

[0019] In one embodiment, the second remote monitoring device is a portable communications device of least one of a mobile phone, a tablet computer or a portable computer.

[0020] In one embodiment, the web server is configured to transmit to at least one of the first and the second remote monitoring devices, status information concerning a wireless relay network associated with the wireless relay device.

[0021] In accordance with a further aspect of the concepts described herein, a system for enabling the remote monitoring of at least one medical device includes a device integrator server in communication with at least one wireless relay device configured to transmit data packets containing information provided by at least one medical device, wherein each data packet includes data identifying medical device data and at least one of a medical device identifier and a patient identifier and a web server configured for providing web pages for receiving at least the medical device data and, subject to verification of the patient identifier and medical device identifier, transmitting the medical device data to first and second remote monitoring devices via a secure internet connection for displaying the medical device data at the first and remote monitoring devices.

[0022] In one embodiment, the system further includes a data manager system coupled to the device integrator server. The data manager system includes at least a device control database.

[0023] In one embodiment, the system further includes a network status server configured for transmitting to at least one of the first or second remote monitoring devices, status information concerning a wireless relay network associated with the wireless relay device.

[0024] In one embodiment, the network status server is located at a different geographic location than the web server.

[0025] In accordance with a further aspect of the concepts described herein, a method for displaying medical device data by a medical device monitoring system, the method including receiving credentials from a user of a first monitoring device and a request from the user for medical device information for a patient to be monitored and verifying the user is authorized to receive the medical device information. In response to verification being achieved, then, (a) identifying, based at least upon the credentials and the request, an address for a secure patient database having information regarding the patient.

[0026] In one embodiment, the method further includes (b) retrieving patient data and associated medical device identification data by a web server from the patient database over a secure communications link and (c) retrieving medical device data from a device control database for at least one medical device according to the retrieved medical device identification data.

[0027] In one embodiment, the method further includes (d) transmitting the retrieved medical device data by the web server for display on the first monitoring device and (e) transmitting at least a portion of the medical device data to a second remote monitoring device for displaying at the second remote monitoring device.

[0028] In one embodiment, the portion of the medical device data transmitted to the second remote monitoring device includes status information concerning a wireless relay network associated with a wireless relay device.

[0029] In one embodiment, the method further includes receiving from the wireless relay module status information concerning a wireless relay network associated with the wireless relay device.

[0030] In one embodiment, the status information concerning a wireless relay network concerns at least one of signal strength, data rates, particular transmission time stamp, number of active relay modules in the wireless relay network, and a unique identifier number for a particular relay module.

[0031] In one embodiment, transmitting the portion of the medical device data to the second remote monitoring device includes encrypting the portion on the portion of the medical device data.

[0032] In one embodiment, transmitting the retrieved medical device data for display on the first monitoring device further includes encrypting the medical device data with a first encryption technique, and wherein transmitting the portion of the medical device data to the second remote monitoring device includes encrypting the portion of the medical device data using a second encryption technique, wherein the first encryption technique differs from the second encryption technique.

[0033] In accordance with a further aspect of the concepts described herein, a system for enabling the remote monitoring of at least one medical device includes an access point in communication with at least one wireless relay device and a separate patient care database node. The access point includes a device integrator server coupled to a database having stored therein medical device data. The access point further includes a secure device server coupled to the device integrator server. The patient care database node includes a secure patient server coupled to a patient database having patient data stored therein. The secure patient server is coupled through a secure link to the secure device server of the access node.

[0034] By separating medical device data and patient data to be respectively stored and managed by access point and patient care database node, certain economies of scale can be achieved by configuring the access point to support a number of different patient care facilities each maintaining its own secure patient care database node to ensure privacy and control of its associated patient data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0035] The invention will become more readily apparent from the Detailed Description of the Invention, which proceeds with reference to the drawings, in which:

[0036] FIG. 1 presents a block diagram of an exemplary remote monitoring system for remotely monitoring medical devices according to the present invention;

[0037] FIG. 2 presents a flow diagram illustrating an exemplary method for registering medical devices with the remote monitoring system according to FIG. 1;

[0038] FIG. 3(a) presents a flow diagram illustrating an exemplary method for retrieving and viewing medical data via the remote monitoring system according to FIG. 1;

[0039] FIGs. 3(b)-3(d) illustrate exemplary screen displays for retrieving and viewing the medical data according to the method of FIG. 3(a);

[0040] FIG. 4(a) presents a flow diagram illustrating an exemplary method for issuing a command to a medical device via the remote monitoring system according to FIG. 1;

[0041] FIG. 4(b) and 4(c) illustrate exemplary screen displays for commanding a medical device according to the method of FIG. 4(a);

[0042] FIG. 5(a) presents a flow diagram illustrating an exemplary method for recognizing and reporting an alert condition according to medical data logged via the remote monitoring system according to FIG. 1;

[0043] FIG. 5(b) illustrates an exemplary screen display for selecting a recipient for receiving an alert message according to the method of FIG. 5(a); and

[0044] FIG. 6 presents a block diagram of an exemplary computer or server device suitable for use in the remote monitoring system according to FIG. 1.

DETAILED DESCRIPTION

[0045] Reference will now be made in detail to exemplary embodiments of the invention, including the best modes contemplated by the inventors for carrying out the invention. Examples of these exemplary embodiments are illustrated in the accompanying drawings. While the invention is described in conjunction with these embodiments, it will be understood that it is not intended to limit the invention to the described embodiments. Rather, the invention is also intended to cover alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

[0046] In the following description, specific details are set forth in order to provide a thorough understanding of the present invention. The present invention may be practiced without some or all of these specific details. In other instances, well-known aspects have not been described in detail in order not to unnecessarily obscure the present invention.

[0047] For the purpose of illustrating the present invention, exemplary embodiments are described with reference to FIGs. 1-6.

[0048] In this specification and the appended claims, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood to one of ordinary skill in the art to which this invention belongs.

[0049] A diagram of an exemplary system 100 for monitoring medical devices in accordance with the present invention is illustrated in FIG. 1. For example, one or more medical devices 10 are provided at a patient facility 20 for monitoring the medical condition and/or administering medical treatment to one or more patients. Patient facility 20 may comprise a critical care health service center (for example, including hospitals, clinics, assisted living centers and the like) servicing a number of patients, a home facility for servicing one or more patients, or a personal enclosure (for example, a backpack) that may be attached to or worn by an ambulatory patient. Examples of medical devices include, but are not limited to, include ventilators, urology devices, energy delivery devices, pulse oximeters, predictive thermometers, tympanic thermometers, patient electrodes, and food pumps.

[0050] Associated with each medical device 10 is an interface circuit 15 that includes a transceiver having one or more of a transmitter and/or a receiver for respectively transmitting and receiving signals in a facility-oriented wireless network 17 such as, for example, a Low-Rate Wireless Personal Area Networks or "LR-WPAN," ZIGBEE network or another low-power personal area network such as a low power Bluetooth network, existing or presently under development or consideration. See, e.g., Houda Labiod et al., *Wi-Fi, Bluetooth, Zigbee and WiMax*, Springer 2010, which is incorporated by reference herein in its entirety. It should be understood that interface circuit 15 may be contained within or disposed external to medical device 10 in accordance with the present invention.

[0051] Also provided within the patient facility 20 are one or more relay modules 30. Each relay module 30 includes a first transceiver for receiving signals from and transmitting signals to the interface circuits 15 in the facility-oriented wireless network 17, and further includes a second transceiver for wirelessly transmitting signals to and receiving signals from an access point 40 via a wireless wide-area network ("WWAN") 52. Suitable WWANs for use with the present invention include, for example, networks based on a Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA) cellular network or associated with the 2G, 3G, 3G Long Term Evolution, 4G, WiMAX cellular wireless standards of the International Telecommunication Union Radiocommunication Sector (ITU-R). See, e.g., Vijay Garg, *Wireless Communications & Networking*, Morgan Kaufmann 2007, which is incorporated by reference herein in its entirety. For compliance with HIPAA regulations, communications over each of the facility-oriented wireless network and WWAN are preferably conducted securely using, for example, a Secure Sockets Layer (SSL) protocol or a Transport Layer Security (TLS) protocol or other cryptographic protocols.

[0052] As illustrated in FIG. 1, the access point 40 useable with the present invention includes an inbound server ("device integration server") 41 that incorporates or otherwise has access to a transceiver for communicating with the relay modules 30 over the WWAN. Medical device data, medical device identifier, and/or patient identifier received by the device integration server 41 over the WWAN is forwarded to a secure device web server 42, which is configured for example to log the received data in association with identification information of the associated medical devices in a device

control database 44. "Medical device data" as generally used herein means data from or about the medical device including, for example, medical device identification, medical device software, medical device settings or status information (including alarm information and/or alarm priority), patient identification information, patient personal identification number(s) "PIN(s)", patient prescriptions, and/or patient medical and/or physiological data as is collected, produced and/or generated by at least one of the medical device and patient identification device; as well as wireless relay network information such as location or status information.

[0053] An outbound web server 43 is configured, for example, to receive and qualify data retrieval requests submitted by one or more of first remote monitoring devices 62 over a broad-band network 50 (for example, over the Internet), and/or second remote monitoring devices 70, 75 over a wired or wireless wide area network. It is advantageous for such requests be made in an encrypted format. Suitable encryption formats useable for such requests may include, for example, formats compliant with the HIPAA regulations described above. For each qualified request, the outbound web server 43 requests associated medical device data or portions thereof to be retrieved from the device control database 44 via the secure device web server 42, requests associated program data for constructing a display page from a metadata and applications database 46, and requests associated patient data to be retrieved from a patient database 66 provided in a patient care database node 60 over a secure link 54 via a secure patient web server 64. The secure link 54 can be implemented, for example as another WWAN using a SSL protocol or a TLS protocol. By separating medical device data and patient data to be respectively stored and managed by access point 40 and patient care database node 60, certain economies of scale can be achieved by configuring the access point 40 to support a number of different patient care facilities each maintaining its own secure patient care database node 60 to ensure privacy and control of its associated patient data.

[0054] In this case, for example, a third party service provider may host the access point 40 to simultaneously support a number of distinct patient and/or home care facilities, thereby eliminating the need for each of these facilities to configure and maintain their own private access point facilities and providing hosting service to each facility that are likely far less than the costs of configuring and maintaining dedicated access point facilities by each care facility provider. It should be noted however that, consistent with

principles of the present invention, access point 40 and patient care database node 60 may nevertheless be integrated into a single access point or node (for example, by a provider of a very large-scale facility provider monitoring many hundreds or thousands of patients). In either case, and as further described herein, the outbound web server 43 provides an interface for authenticated clinicians or other monitoring personnel to retrieve patient and medical device data from each of the patient care database node 60 and the access point 40 in a convenient and transparent manner such that the details of the configurations and operation of the access point 40 and patient care database node 60 are of no consequence to the clinicians or other monitoring personnel.

[0055] The first remote monitoring devices 62 are intended to be used by healthcare providers such for example, clinicians, physicians, technicians, nurses and other healthcare specialists monitoring patients associated with medical devices 10. Suitable first remote monitoring devices 62 may include, for example, desktop or laptop computers, tablet computer smart or other mobile phones, or other fixed or portable display devices. The second remote monitoring devices 70, 75 are advantageously intended to be used by caregivers and/or relatives of the patient such as parents, located proximate the patient such as in a homecare environment or small healthcare facility, or nurses at a larger healthcare facilities, e.g., hospitals. Suitable second remote monitoring devices 70, 75 likewise may include, for example, desktop or laptop computers, tablet computer, smart or other mobile phones, or other fixed or other portable communication devices.

[0056] In addition, the outbound web server 43 is depicted coupled to a network status server 80, which monitors the status of the facility-oriented wireless network 17 and associated medical devices 10. The network status server 80 is intended to provide status information concerning the facility-oriented wireless network 17 and associated medical devices 10 to the outbound web server 43. Exemplary status information concerning the facility-oriented wireless network 17 includes, for example, signal strength, data rates, particular transmission time stamps between modules comprising the network 17, number active relay modules in the network 17, unique identifier number for a particular relay module of the network 17.

[0057] The network status server 80 may be implemented in hardware or software running on an application specific or general purpose processor or computer, as part of or separate from the outbound web server 43. In addition, the network status server 80 is

shown coupled to the outbound web server 43 for ease of illustration and discussion purposes only. The network status server 80 may be coupled to any component or network of the access point 40 or facility-oriented wireless network 17 in accordance with the invention.

[0058] In FIG. 1, upon retrieving the requested medical device data and patient data from the patient care database node 60, the outbound web server 43 then proceeds to format and transmit the retrieved medical device data and patient data (and /or provide status information concerning the facility-oriented wireless network 17 and associated medical devices 10) as respective webpages or other formats for display by corresponding first and second remote monitoring devices 62, 70, 75 according to the retrieved program data. It is possible for the webpages or other formatted information for display to include the same or differing content and format for the intended remote monitoring device user depending upon the retrieved program data. For example, the detailed medical device data provided to and displayed on a first remote monitoring devices 62 for a clinician may differ from the less detailed information provided to and displayed on a second remote monitoring devices 70 monitored by a parent or visiting nurse or other healthcare professional in a homecare environment. The status information concerning the facility-oriented wireless network 17 and associated medical devices 10 may advantageously be provided to first and/or second remote monitoring devices 62, 70 and 75 in the same or different encrypted formats as may be deemed appropriate.

[0059] In addition, and as will be further described herein, the device integration server 41 of FIG. 1 is configured to transmit information and commands to the relay modules 30, for example, for transmitting medical device or alert messages to other WWAN-reachable nodes (for example, cellular telephones of emergency attendants), and/or transmitting operating commands and/or software or firmware updates to the medical devices 10 via the interface circuits 15 and facility-oriented wireless network 17.

[0060] Further, in addition to monitoring and sending commands to medical devices, the device integration server 41 may also be configured to receive and analyze patient metric information from the secure patient web server 64 via the outbound web server 43 and secure device web server 42, or by an alternate and direct secure data link to the secure patient web server 64 in order to prevent unsafe medical device usage based upon the patient metrics information. It is possible for a database (not depicted)

accessible, for example, by the device integration server 41 and/or device web server 42, to store various safe and unsafe operating parameters and conditions for performing such analysis. In this manner, the device integration server 41 would function as an additional failsafe for preventing operating errors that could result in patient harm.

[0061] For example, in the case that the patient metric information indicates that an enteral feeding pump is associated with a neonate, the device integration server 41 may act, for example, to (1) discard remote monitoring commands programming large bolus or excessive feeding rates that could be harmful to a young child; and (2) provide a warning message or other notification to the user of the likely unsafe usage condition that may result by implementation of such comment. Alternatively, if the patient metric information indicates that a specific feeding rate or bolus amount has been prescribed by a doctor or clinician, then the device integration server may act to discard remote monitoring commands programming a rate or bolus that deviates from the prescription.

[0062] FIG. 2 illustrates a flow diagram of one exemplary method 200 in accordance with the invention for registering medical devices 10 with the system 100 of FIG. 1. The method 200 begins at step 202, at which an authorized technician or other personnel having access to one of the remote monitoring devices 62, 70, 75 provides authenticating credentials (for example, a recognized log-in and password) to the outbound web server 43, and the web server responds by transmitting a device set-up screen to the remote monitoring device 62, 70, 75 requesting medical device identifying information and associated patient identifying information.

[0063] At step 204, the outbound web server 43 preferably queries the metadata and application database 46 according to one or more of identifying information for the technician and/or identifying information for the patient to identify an associated patient care database node 60 from a plurality of patient care database nodes for the patient and record a destination address for the associated patient care database node 60 in the metadata and application database 46 in association with the identifying data for the medical device 10 and/or identifying information for the patient. Identifying information for the patient is preferably generated anonymously (for example as a random number), and transmitted at step 206 to the patient care database node 60 for association with securely-stored patient identifying information. At step 208 of the method 200 of FIG. 2, the outbound web server 43 requests that the secure device web server 42 assign an area of

the device control database 44 for logging associated medical device data for the medical device 10 as it is received by the device integration server 41, such that it can be later retrieved by the outbound web server 43 upon receiving an authorized request from an authenticated user operating one of the remote monitoring devices 62, 70, 75.

[0064] It should be readily understood by one skilled in the art that step 204 of method 200 for identifying and storing the address of the patient care database node 60 may be omitted in accordance with the invention if a single patient care database node is utilized with system 100 of FIG. 1.

[0065] FIG. 3(a) presents a flow diagram illustrating one exemplary method 300 in accordance with the invention for retrieving and viewing medical device data on a remote monitoring device 62, 70, 75 for a registered medical device 10 according to the system of FIG. 1. The method 300 begins at step 302 with a first authorized user having access to one of the first remote monitoring devices 62 provides authenticating credentials (for example, a recognized log-in and password) to the outbound web server 43. In addition, in step 302, a second authorized user having access to one of the second remote monitoring devices 70, 75 likewise provides respective authenticating credentials to the outbound web server 43

[0066] At step 304, based on verification of the authenticating credentials of the first and second authorized users, the outbound web server 43 queries the metadata and applications database 46 to identify the address of patient care database node(s) 60 to which the respective first and second authorized users are entitled to obtain access, and at step 306, requests data from the patient care database node 60 relating to at least one identified patient for which the first and second user are respectively authorized to view medical device data, including for example a listing of medical devices 10 which are presently associated with the identified patient, and/or status information of the facility-oriented network 17. . It should be readily understood that different authenticated users will likely have different levels of sophistication and skill for which a corresponding access level may be associated with their authentication account or status which may further be used, for example, to limit or expand the type and/or extent of medical device data that may be transmitted to the remote monitoring devices for such authenticated users.

[0067] At step 308 of the method 300 of FIG. 3(a), the outbound web server 43 queries the device control database 44 via the secure device web server 42 for status information to determine which of the listed medical devices are presently active according to the data logged by the device control database 44. It should be noted that one or more of a medical device 10, its associated interface device 15, an associated wireless relay module 30 and/or the device integration server 41 may be programmed to provide data from the medical device 10 to the device integration server 41 at predetermined, preset intervals or otherwise, which can then be provided to server 43 in response to inquiries therefrom.

[0068] Upon obtaining the status information, the outbound web server 43 prepares respective display pages with encrypted medical device data, according for example to display information retrieved from the metadata and applications database 46, to display listings of medical devices 10 available for monitoring by respective authorized users at the remote monitoring devices 62, 70, 75. FIG. 3(b) presents a first exemplary screen display 320 to the remote monitoring devices 62, 70, 75 that provides an array of medical devices 10 available for monitoring according to device type. For example, in the screen display 320 of FIG. 3(b), available device types include ventilators 321, urology devices 322, energy delivery devices 323, pulse oximeters 324, predictive thermometers 325, tympanic thermometers 326 and food pumps 327. Each of the device types 321-327 in FIG. 3(b) is presented with an identifying label (for example, label 321A) and an identifying image (for example, image 321B) for ease of recognition.

[0069] Once a device type is selected by a user (for example, in response to an associated mouse-over or mouse-click executed by the authorized user), a second exemplary screen display 330 as illustrated by FIG. 3(c) may preferably be transmitted by the outbound web server 43 for display at the remote monitoring devices 62, 70 or 75. In the display 330, labels 337A are provided in association with images 337B in order to identify individual food pumps (for example, by patient and/or by logical or physical location). Medical devices 10 that are unavailable may for example preferably be depicted with a label 337A' ("Off Line") and an image 337B' (depicting the device with a slash or cross applied over the image or shaded or shadowed) that distinguish the unavailable medical devices 10 from available medical devices 10.

[0070] Once an individual device is selected by the first or second user (for example, once again, in response to an associated mouse-over or mouse-click executed by the authorized user), a third exemplary screen display 340 as illustrated by FIG. 3(d) may preferably transmitted by the outbound web server 43 for display at the corresponding remote monitoring device 62, 70, 75. In the display 340, for example, device information of the medical device 10 (in this case, a food pump) is displayed in a screen 347A preferably recreating a current screen generated and displayed by the medical device 10. In addition, the screen display 340 includes any of a panel 347B providing identifying information for the medical device 10 (in this case, a pump location), a panel 347C for displaying a message indicating a current error condition of the pump, and an icon button 347D for selecting an alternate "status" mode of the screen display 340. The screen display 340 also includes a control icon button 347E for selecting a system set-up screen display, and a control icon button 347F for enabling device control from the remote monitoring device 62. For example, upon selecting the control icon 347F, the screen display 340 may preferably be refreshed to include the medical devices screen 347A and one or more operable buttons that mimic the appearance of control buttons on the medical device. The control button features are described in greater detail below in relation to FIGs. 4(b) and 4(c).

[0071] It should be readily understood that exemplary computer screen images 320, 330 and 340 and corresponding navigation depicted by FIGs. 3(b), 3(c) and 3(d) are for illustration purposes only and that many other user screen images displays and interface tools may be utilized for carrying out the present invention including, for example, computer screens that depict accessible medical devices by other means than device type as illustrated in FIG. 3(b). For example, as a suitable alternative to the screen image 340 of FIG. 3(d) that conveys information from a single medical device, it is possible to implement displays that provide information from multiple medical devices. In addition, it should be readily understood that the outbound web server 43 will preferably be operable to prepare display pages with encrypted medical device data for display on any of a wide variety of display devices (including, for example, workstations, personal computers, tablet devices including tablet computers, and display-based mobile devices including personal digital assistants, smartphones, portable game systems and the like.

[0072] It should also be readily understood that the computer screen images to be available to first and second users of the first and second remote monitoring devices may be different depending upon whether such user is a clinician, nurse, patient relative or other caregiver, i.e., dependent on level of entitlement of the particular authorized user. For example, a display for a clinician at a first remote monitoring device 62 may enable the clinician to adjust the settings of a subject medical device 10, in contrast to a display for a second remote monitoring device 70, 75 used by a patient relative, which depicts only fundamental information from the medical device data with no option for the patient relative to adjust the medical device settings via the second remote monitoring device 70, 75. Likewise, different encryption methods or formats may be employed for medical device data transmitted to the first remote monitoring device 62 than the second remote monitoring device 70, 75.

[0073] FIG. 4(a) presents a flow diagram illustrating an exemplary method 400 in accordance with the invention for issuing a command to a medical device 10 via the system 100 according to FIG. 1. The method 400 begins at step 402 with an authorized user adjusts an operating parameter, such as a clinician (also referred to as a "authorized clinician" or "user" herein) logging into the outbound web server 43 using a first remote monitoring device 62 and navigating to the device screen display 340 of FIG. 3(d) (for example, as described above with reference to FIGs. 3(a)-3(d)). At step 404, the clinician proceeds to select the "Enable Full Control" button 347F of FIG. 3(d) to initiate an operational command directed to the medical device 10, and is preferably provided with a request for authentication pertaining in particular to the patient associated with the medical device 10. At step 406, patient authentication information provided by the clinician is forwarded by the outbound web server 43 to a patient care database node 60 according to a patient care database node address stored by the metadata and applications database 46 in association with the clinician, and the clinician is authenticated for the patient by the outbound web server 43 upon receipt of an authentication confirmed message from the patient care database node 60.

[0074] Upon receipt of the patient authentication, a control request is forwarded by the outbound web server 43 at step 408 to the secure device web server 42 to be logged in the information record of the device control database 44 that is associated with the medical device 10 (and optionally, with an anonymous ID for the patient). At step 410, the secure

device web server forwards the control request, such as an encrypted control request, to the device integration server 41, which transmits an associated device control command over the secure WWAN 52 for receipt by an associated wireless relay module 30 at step 412. The wireless relay module 30 wirelessly communicates the command to the medical device 10 via an associated device interface 15, and awaits a reply confirming execution of the command transmitted by the device interface 15.

[0075] At step 414, the device integration server 41 receives an update message from the wireless relay module 30 via the secure WWAN 52 which confirms that the command was executed by the medical device 10. At step 416, the device integration server 41 forwards the update message to the secure device web server 42 to be logged in the information record of the device control database 44 that is associated with the medical device 10. Optionally, and preferably, the secure device web server 42 forwards information pertaining to the update message to the outbound web server 43, and the outbound web server 43 prepares an updated display screen that is securely transmitted to the remote monitoring device 62 to indicate that the command has been executed.

[0076] Alternatively, at step 404, the authenticated clinician may select the "System Setup" control icon button 347E to perform a command other than an operational command directed to the medical device 10. FIG. 4(b) illustrates a display screen 450 that is presented to the clinician upon selecting the control icon button 347E. The display screen 450 includes a number of icon buttons that may be selected by the clinician (for example, as the result of a mouse-over or mouse-click initiated by the clinician) to select a specific setup command. For example, icon button 451 may be selected to initiate a command for providing identification information of the medical device 10. Icon button 452 may be selected to provide text paging in response to an alert condition, as is further described herein. Icon button 453 may be selected to initiate a software or firmware download for updating the medical device 10.

[0077] Icon button 454 may be selected to initiate a diagnostic test of the medical device 10. FIG. 4(c) illustrates an exemplary display screen 460 that may be displayed to the clinician upon selection of the icon button 454. Via the display screen 460 of FIG. 4(C), the clinician may select one or more of (including a progression of) a series of diagnostic tests 461 directed to components of the medical device (for example, including power components, memory components, alarm components and the like). Alternatively

and/or in addition, the clinician may select one or more of a series of performance statistics 462 to be gathered and displayed (for example, including various device error statistics such as feed error, rotor error and flush error rates for a food pump). In addition, perhaps most usefully before issuing a software and/or firmware download command, the clinician may select a version number test 463 to obtain version identifying information for the software and/or firmware (preferably including, for example, a software and/or firmware download history). Optionally, processes for performing the diagnostic tests 461, preparing the performance statistics 462 and identifying the software and/or firmware version number 463 may run automatically without specifically being selected by the clinician, with a complete reporting of all results on the display screen.

[0078] In a similar manner to that performed by the method of FIG. 4(a), it is possible to issue a bandwidth priority command or instruction to a relay module, such as relay module 30 of FIG. 1, for the relay module to grant priority for relaying information received from a particular medical device relative to other medical devices that may send or receive communications via this relay module. For example, it would be advantageous to provide greater bandwidth priority to a critical care device such as a ventilator supporting the breathing function of a patient relative to a weight scale or thermometer. It is also possible to a number of bandwidth priority levels assignable to respective medical devices based upon, for example, the critical nature of the data or function provided by such devices.

[0079] Referring again to FIG. 4(b), icon button 455 may be selected to enable the clinician to specify data transfer rates, priorities and other parameters relating to the wireless transceiver of the interface device associated with the medical device. Icon button 456 may be selected to provide the clinician with the an alarm history, event history and other information as has been logged for example for the medical device in the device control database 44 of FIG. 1.

[0080] It should be readily understood that the method 400 for remotely issuing a command to a medical device 10 was described with respect to a user of a first remote monitoring device 62 and not a user of the second remote monitoring 70, 75 because as described for example throughout this application, it is assumed that the user of the first remote monitoring device 62 is a clinician, technician or other highly-skilled healthcare professionals, while the user of the second remote monitoring device 70, 75 may be a

patient relative or caregiver of lesser skill. Nevertheless, the method 400 is likewise useable to enable a user of the second monitoring device 70, 75 to also control particular settings of the medical device 10.

[0081] FIG. 5(a) presents a flow diagram illustrating one exemplary method 500 in accordance with the invention for recognizing and reporting an alert condition according to medical device data (including the status of the facility-oriented network 17) logged via the system 100 according to FIG. 1. The method 500 begins at step 502 with the transmission of an alert message by a wireless relay module 30 over the secure WAN 52 to the device integration server 41. In this case, the wireless relay module 30 is configured to analyze (such as by detecting flag or status information or comparing message data to information stored in an associated database) a message type of a message transmitted by an associated medical device 10 to determine that the message is an alert message, and to transmit the message to the device integration server 41 upon determining that the message is an alert message (for example, as a priority message). Alternatively, the wireless relay module 30 may simply queue all messages for transmission to the device integration server 41 in order upon receipt, and rely upon the device integration server 41 to analyze an associated message type to determine that a message is an alert message.

[0082] Upon determining that the transmitted message is an alert message, the device integration server 41 proceed, at step 503, to log the message in the device control database 44, and at step 504, invokes a text messaging application that retrieves text messaging numbers associated with identifying information of the medical device 10 and/or anonymous patient identifying information. The determination of whether the transmitted message is an alert message may be carried out by, for example, detecting an alert flag or trigger identifier in the message or scanning the message for other information indicative of an alert condition. The text messaging application may preferably retrieve the text messaging numbers by querying the metadata and applications database 46 to identify the address of an associated patient care database node 60, and either making a direct request or instructing the outbound web server 43 to request the text messaging numbers from the associated patient care database node 60.

[0083] At step 506, the device integration server 41 sends one or more messages including the retrieved text messaging numbers and text message information according to the alert message to one or more wireless relay modules 30 over the secure WWAN 52.

At step 508, the one or more wireless relay modules 30 transmit the text message information addressed to the text messaging numbers over one or more of the secure WWAN 52 and/or the facility-oriented wireless network 17 to complete the method 500.

[0084] FIG. 5(b) illustrates a "Text Paging" 452 screen display 550 that may be invoked, for example, by using the method 400 of FIG. 4(a) for issuing a command to a medical device 10. Specifically, and with particular reference to FIGs. 3(d) and 4(b), the text paging screen 550 is displayed at the first remote monitoring device 62 of an authenticated clinician upon the clinician's selection of the "System Setup" icon button 347e of the screen display 340, and thereafter upon the clinician's selection go the "Text Paging" icon button of the screen display 450. Likewise, it is possible for the paging screen 550 of FIG. 5(b) to be displayed on a second remote monitoring device 70, 75 for completion by an authorized user, such as a patient relative or other caregiver. As illustrated in FIG. 5(b), the "Text Paging" screen display 550 include a listing of one or more names 551 of individuals responsible for responding to alert messages of at least two types: "Error Messages" 553, which may for example indicate a malfunction of the medical device 10, and/or "Info Messages" 554, which may for example indicate a significant patient health condition (for example, a patient respiration rate below a preset minimum rate specified for a ventilator device 321 of FIG. 3(b)).

[0085] The information retrieved by the outbound web server 43 to prepare this display is preferable retrieved from the patient care database node 60, by providing on one or more of identifying information for the medical device 10 and/or anonymous patient identifying information stored in the device control database 44. Upon recognizing an alert message for the medical device 10, the information provided on the "Text Paging" screen display may be retrieved by the device integration server 41 by querying the metadata and applications server 46 to retrieve address information for the patient care database node 60, and forwarding a text paging information request to the patient care database node 60 based upon one or more of identifying information for the medical device 10 and/or anonymous patient identifying information stored in the device control database 44. The recognition of whether the received message from the medical device 10 is an alert message may be carried out by, for example, detecting an alert flag or trigger identifier in the message or scanning the message for other information indicative of an alert condition.

[0086] It should be readily understood that the use of communicating alert messages using text messaging in Figs. 5(a) and 5(b) is for ease of illustration purposes only and that such alerts may be communicated in other ways in accordance with the present invention including email, audio messages via telephone calls, as well as any other wired and/or wireless text, audio, or multimedia based communication services receivable by, for example, by a smart phone or computer tablet software application or "App."

[0087] FIG. 6 shows an illustrative computer system 600 suitable for implementing server and computer components of the present invention (for example, including device integration server 41, secure device web server 42, outbound web server 43, and secure patient web server 64). The computer system 600 as described herein may comprise, for example, a personal computer running the WINDOWS operating system, or a server computer running, WINDOWS Server, LINUX or another UNIX-based operating system. Alternatively, the computer system 600 described herein may comprise a mobile device, tablet devices or computers, or information appliance running, for example, an operating system in the group including Symbian , Android, Apple iOS, Blackberry, Microsoft Windows Phone, Linux, Palm/HP WebOS, BADA, MAEMO and MEEGO. The above-described methods carried out by the server and computer components of the present invention may be implemented on the computer system 600 as stored program control instructions directed to control application software.

[0088] Computer system 600 includes processor 610, memory 620, storage device 630 and input/output devices 640. One of the input/output devices 640 may preferably include a display 645. Some or all of the components 610, 620, 630 and 640 may be interconnected by a system bus 650. Processor 610 may be single or multi-threaded, and may have one or more cores. Processor 610 executes instructions which in the disclosed embodiments of the present invention are the steps described, for example, in one or more of FIGs. 2, 3(a), 4(a) or 5(a). These instructions may be stored in one or more of memory 620 or in storage device 630. Information may be received and output using one or input/output devices 640. Memory 620 may store information and may comprise a computer-readable medium, such as volatile or non-volatile memory. Storage device 630 may provide storage for system 600 including for the example, the previously described database, and may be a computer-readable medium. In various aspects, storage device 630

may be one or more of a flash memory device, a floppy disk drive, a hard disk device, and optical disk device, and/or a tape device.

[0089] Input devices 640 may provide input/output operations for system 600. Input/output devices 640 may include one or more of a keyboard, a pointing device, and/or microphone. Input/output devices 640 may further include a display unit for displaying graphical user interfaces, a speaker and a printer and any of a number of other serial devices (for example, configured as Universal Serial Bus (USB)-based devices

[0090] It should of course, be understood that while the present invention has been described with respect to disclosed embodiments, numerous variations are possible without departing from the spirit and scope of the present invention as defined in the claims.

[0091] Moreover, it is intended that the scope of the present invention include all other foreseeable equivalents to the elements and structures as described herein and with reference to the drawing figures. Accordingly, the invention is to be limited only by the scope of the claims and their equivalents.

We claim:

1. A system for enabling the remote monitoring of at least one medical device, the system comprising:

a device integrator server in communication with at least one wireless relay device, wherein said wireless relay device is configured to transmit data packets containing information provided by at least one medical device, wherein each said data packet includes identifying medical device data and at least a medical device identifier or a patient identifier;

a data manager system coupled to said device integrator server, said data manager system comprising at least a device control database, and

a web server configured for providing web pages for receiving at least the medical data and, transmitting the medical device data to a first remote monitoring device via a secure internet connection for displaying the medical device data at the first remote monitoring device; and transmitting at least a portion of the medical device data to a second remote monitoring device for displaying the portion of the medical device data at the second remote monitoring device.

2. The system of claim 1 wherein said web server is configured for verifying the patient identifier and medical device identifier before transmitting the medical device data to the first remote monitoring device.

3. The system of claim 1 wherein said web server is configured to transmit the portion of the medical device data to the second remote monitoring device by at least a wireless data link.

4. The system of claim 3 wherein said wireless data link is over a wireless mobile data network.

5. The system of claim 1 wherein the second remote monitoring device is a portable communications device of least one of a mobile phone , tablet computer and portable computer.

6. The system of claim 1 wherein said web server is configured to transmit to at least one of the first and the second remote monitoring devices, status information concerning a wireless relay network associated with the wireless relay device.

7. A system for enabling the remote monitoring of at least one medical device, the system comprising:

a device integrator server in communication with at least one wireless relay device, wherein said wireless relay device is configured to transmit data packets containing information provided by at least one medical device, wherein each said data packet includes data identifying medical device data and at least one of a medical device identifier and a patient identifier ;

a data manager system coupled to said device integrator server, said data manager system comprising at least a device control database,

a web server configured for providing web pages for receiving at least the medical device data and, subject to verification of the patient identifier and medical device identifier, transmitting the medical device data to first and second remote monitoring devices via a secure internet connection for displaying the medical device data at the first and remote monitoring devices; and

a network status server configured for transmitting to at least one of the first or second remote monitoring devices, status information concerning a wireless relay network associated with the wireless relay device.

8. The system of claim 7 wherein said network status server is located at a different geographic location than the web server.

9. A method for displaying medical device data by a medical device monitoring system, the method comprising:

receiving credentials from a user of a first monitoring device and a request from said user for medical device information for a patient to be monitored;

verifying said user is authorized to receive the medical device information; and

if verification is achieved, then

(a) identifying, based on at least said credentials and said request, an address for a secure patient database having information regarding said patient;

(b) retrieving patient data and associated medical device identification data by a web server from said patient database over a secure communications link;

(c) retrieving medical device data from a device control database for at least one medical device according to said retrieved medical device identification data;

(d) transmitting said retrieved medical device data by said web server for display on said first monitoring device; and

(e) transmitting at least a portion of the medical device data to a second remote monitoring device for displaying at the second remote monitoring device.

10. The method of claim 9, wherein transmitting at least a portion of the medical device data to a second remote monitoring device comprises transmitting at least status information concerning a wireless relay network associated with a wireless relay device to the second remote monitoring device.

11. The method of claim 9, further comprising receiving, from said wireless relay module, status information concerning a wireless relay network associated with the wireless relay device.

12. The method of claim 9, wherein the status information concerning a wireless relay network concerns at least one of signal strength, data rates, particular transmission time stamp, number of active relay modules in the wireless relay network, and a unique identifier number for a particular relay module.

13. The method of claim 9 wherein transmitting the portion of the medical device data to the second remote monitoring device comprises encrypting said portion on the portion of the medical device data.

14. The method of claim 9 wherein the step of transmitting the retrieved medical device data for display on the first monitoring device further comprises encrypting said medical device data with a first encryption technique, and wherein said step of

transmitting the portion of the medical device data to the second remote monitoring device comprises encrypting the portion of the medical device data using a second encryption technique, wherein the first encryption technique differs from the second encryption technique.

15. A system for enabling the remote monitoring of at least one medical device, the system comprising:

at least one wireless relay device configured to communicate with the at least one medical device;

an access point in communication with the at least one wireless relay device, said access point including a device integrator server coupled to a database having stored therein medical device data and a secure device server coupled to said device integrator server;

a patient care database node separate from said access point, said patient care database node including a secure patient server coupled to a patient database having patient data stored therein; and

a secure link coupled between said secure patient server and said secure device server of said access node.