MobileCare™ Monitor System

Operator's Manual

Contents

Warnings and Precautions

Contraindications

- Do not use the device in an MR environment.
- Do not use this device in an explosive atmosphere or in the presence of flammable anesthetics or gases.
- This device is not defibrillation proof per IEC 60601-1:1990 clause 17h.

Warnings

- Use within its designated range.
- This device is intended only as an adjunct in patient assessment. It must be used in conjunction with other methods of assessing clinical signs and symptoms.
- Operation of this device below the minimum amplitude of 0.3% modulation may give inaccurate results.
- The use of batteries other than those specified in these instructions may result in increased electromagnetic emission and/or decreased immunity of this device.
- This device should not be used adjacent to or stacked with other equipment. If adjacent or stacked use cannot be avoided the device should be observed carefully to verify normal operation.

Cautions

- Inspect the device at least every 6 to 8 hours to ensure correct device alignment and skin integrity. Patient sensitivity to the device may vary due to medical status or skin condition.
- Factors that may degrade the performance or affect the accuracy of the measurement, include the following:
  - excessive light, such as sunlight or direct home lighting
  - excessive motion
  - moisture in the device
  - improperly applied device
- Do not sterilize, autoclave, or immerse this device in liquid.
- Do not use caustic or abrasive cleaning agents or any cleaning products containing ammonium chloride.
- This equipment complies with IEC 60601-1-2:2004 for electromagnetic compatibility for medical electrical equipment and/or systems. This standard is designed to provide reasonable protection against harmful interference in a typical medical installation. However, because of the proliferation of radio-frequency transmitting equipment and other sources of electrical noise in health care and other environments, it is possible that

high levels of such interference due to close proximity or the strength of a source might disrupt the performance of this device. Medical electrical equipment needs special precautions regarding EMC, and all equipment must be installed and put into service according to the EMC information specified in this manual.

- Portable and mobile RF communications equipment can affect medical electrical equipment.
- Batteries may leak or explode if used or disposed of improperly. Do not remove or attempt to change the batteries in any manner. This is only to be performed by an AFrame Digital authorized representative.
- Follow local, state, and national governing ordinances and recycling instructions regarding disposal or recycling of the device and device components, including batteries.
- In compliance with the European Directive on Waste Electrical and Electronic Equipment (WEEE) 2002/96/EC, do not dispose of this product as unsorted municipal waste. This device contains WEEE materials. Please contact your distributor regarding take-back or recycling of the device.

Precautions while using MobileCare™ Monitor

Read this manual carefully before using the MobileCare™ Monitor System or its associated components. Follow these precautions:

- Do not use the MobileCare™ Monitor System as a substitute for usual and customary resident supervision. The MobileCare™ Monitor System is intended to assist caregivers in providing proper care to individuals.

- Discontinue use of myPHD if the patient demonstrates any allergic reaction or other intolerance to the device.

- General operation of the MobileCare™ Monitor System may be affected if used in a strong electromagnetic field environment.

- Do not use the system if any component is damaged.

- Caution the residents against causing impacts to myPHD. Intended or unintended impact of myPHD may trigger alerts.

- Do not immerse the MobileCare™ Monitor or its components in water or any other liquid.

- Do not use caustic or abrasive cleaning agents for the MobileCare™ Monitor or its components.

- Do not remove any covers or open any of the components of the MobileCare™ Monitor System. There are no operator serviceable parts within the MobileCare™ Monitor System.

- Follow local governing ordinances and recycling instructions regarding disposal or recycling of the MobileCare™ Monitor and its components, including batteries.

- Batteries may leak or explode if used or disposed of improperly.

About this manual

Audience

The *MobileCare™ Monitor Operator's Manual* is intended for the operators of MobileCare™ Monitor and its components, that is, the caregivers, nurses, and administrative staff of the care giving facility.

What you will find in this manual

This manual describes —

- How the MobileCare™ Monitor System works.
- How to use the myPHD wristwatch to send alerts.
- How to use the CareStation™ software to respond to alerts.

Use the following table to quickly find information in this manual:

To find out about:	Go to:
How the MobileCare™ Monitor System works	2.0 System Overview
How to use myPHD and the CareStation™ software	3.0 Operating Procedures
How to solve problems with the functioning of myPHD and PANDA	4.0 Troubleshooting
The security features of the MobileCare™ Monitor System	5.0 Security
The warranty details, service facilities, and specifications of the MobileCare™ Monitor System	Appendix

Symbols used in this manual

The following symbols have been used in this manual:

WARNING: Warnings alert you about instructions or procedures that could be hazardous, if not followed properly.

NOTE: Notes point out something important or useful.

Conventions used in this manual

The following conventions are used in this manual.

This type of text:	Is used for:
Bold	Button names
Italics	Emphasis

Assumptions

- We assume that the MobileCare™ Monitor System is already installed by a qualified representative of AFrame and is running on your facility's network.

- This guide is intended for the operators of the MobileCare™ Monitor System, that is, the caregivers, nurses, and administrative staff of the care giving facility.

1.0 Introduction

The MobileCare™ Monitor System is a wireless based health and alert monitoring system to support caregivers in continuing care retirement communities and assisted living settings. The system has been designed primarily to monitor elderly residents who require a greater level of assistance on a round-the-clock basis. For monitoring purposes, residents wear a specially designed watch that is part of the MobileCare™ Monitor System. The system sends designated alerts (*see Figure 1.1*) from these residents to administrators and healthcare providers (or caregivers) of multi-resident care facilities. These alerts are designed to elicit a quick response from the caregivers (*see Figure 1.2*). In addition, caregivers can track the location of the residents within the premises of the healthcare facility.
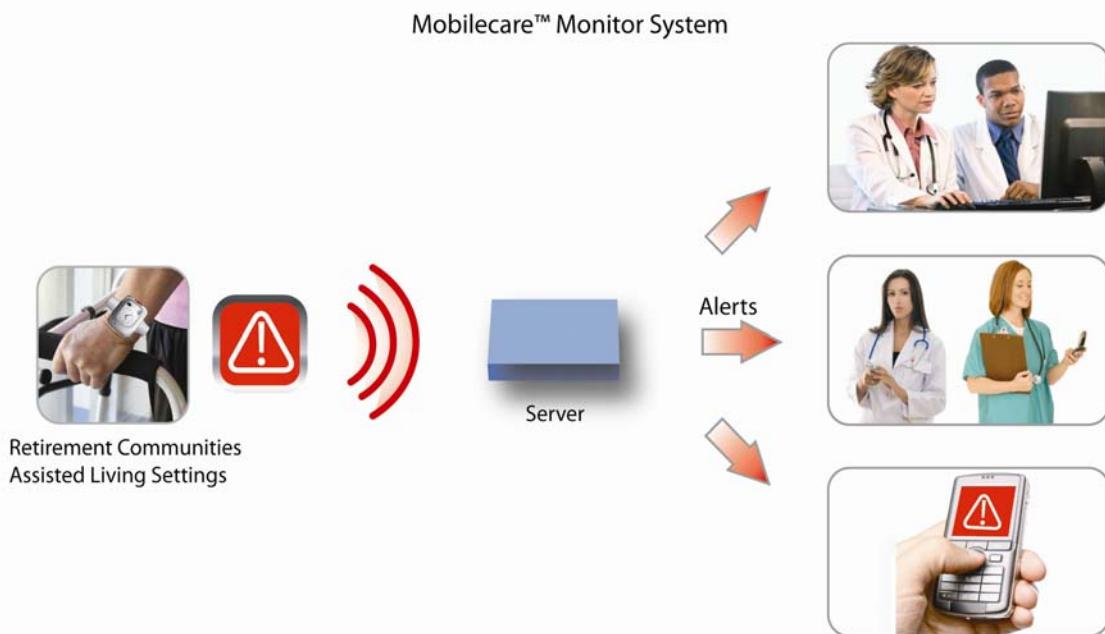
Figure 1.1 Sending alerts to the healthcare professionals via the MobileCare™ Monitor System

1
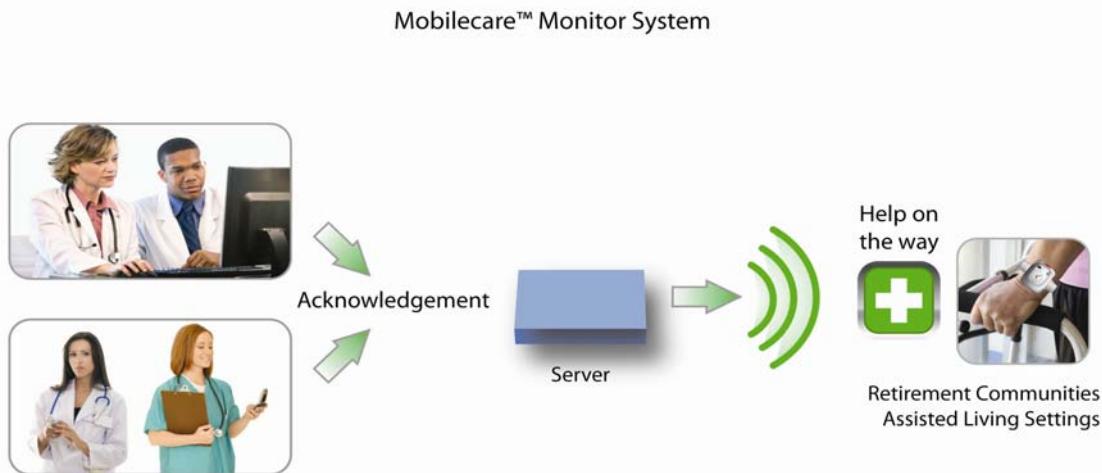
Figure 1.2 Healthcare professionals acknowledge the alerts via the MobileCare™ Monitor System

The MobileCare™ Monitor System is intended only as an adjunct in patient assessment and care. It must be used in conjunction with other methods of assessing the health and wellness in individuals and symptoms. The system is not intended to provide automated treatment decision, nor is it to be used as a substitute for professional healthcare judgment. All patient medical diagnosis and treatment are to be performed under the direct supervision and oversight of an appropriate healthcare professional.

2

2.0 System Overview

The MobileCare™ Monitor System helps healthcare professionals and caregivers to provide wireless monitoring services for independent and ambulatory residents in retirement communities or assisted living settings. The MobileCare™ Monitor System is capable of monitoring elderly residents on a continuous basis (24x7). The system is primarily designed to monitor alerts from these individuals and transmit this data to servers for storage and processing. The main applications of the MobileCare™ Monitor System are:

- Residents can send emergency and assistance needed alerts to caregivers.
- Caregivers can keep track of the location of the residents within the premises.
- Caregivers are provided impact detection alerts.

The user interface between a monitored individual and the MobileCare™ Monitor System is a wireless personal help device (myPHD) or "watch" that is worn on an individual's wrist. This watch is a non-intrusive and form-friendly portable alerting device that transmits data wirelessly to a gateway and server via a wireless mesh network.

The MobileCare™ Monitor System consists of the following components (*see Figure 2.1*):

- **Personal Help Device or myPHD** (also called watch)
- **Wireless Network** — consisting of a PANDA X4 wireless gateway and a mesh network of XBee wireless wall routers
- **Secure Server** — runs the CareStation™ software, stores data, and analyzes trends in resident data
- **CareStation™ Software** — an application program that provides a graphical user interface to allow the caregivers to respond to myPHD alerts. It also integrates the facility map that provides resident location information to the caregivers.
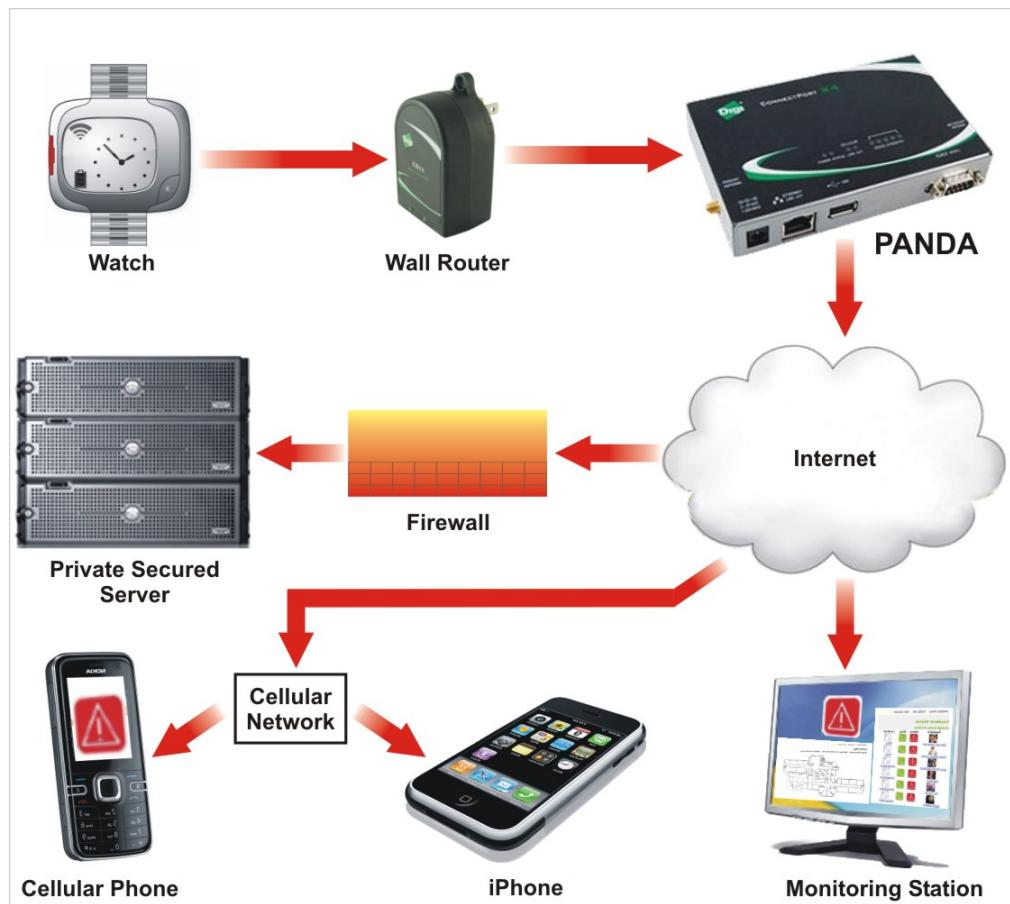
Figure 2.1 Different components of the MobileCare™ Monitor System

2.1 How the MobileCare™ Monitor System Works

Figure 2.2 shows how the myPHDs interact with the wireless network. The wireless network consists of a PANDA X4 gateway and XBee routers that are strategically located inside the individual rooms as well as at other locations of the facility.

The system uses the ZigBee (see "What is ZigBee?" below) mesh network to allow individuals to be mobile within the network. Data is transmitted between the watch and the XBee units through a message-based protocol over a ZigBee mesh network. The data is transferred between the PANDA X4 gateway and the server through a secure HTTP protocol. The caregivers receive alerts via a secure Internet browser, cell phones, PDAs, or other web-enabled phones such as the iPhone. The system can also send healthcare related information to administrators and other healthcare providers for analyzing and archiving purposes.

4

What is ZigBee?

ZigBee is the name given to a set of high-level wireless communication protocols maintained by a group of companies known as the ZigBee Alliance. It is a low-cost, low-power, wireless networking standard based on the IEEE 802.15.4 specifications. The devices using ZigBee form a mesh network, where each device connects wirelessly to the next. ZigBee uses very little power therefore is ideal for small networks.
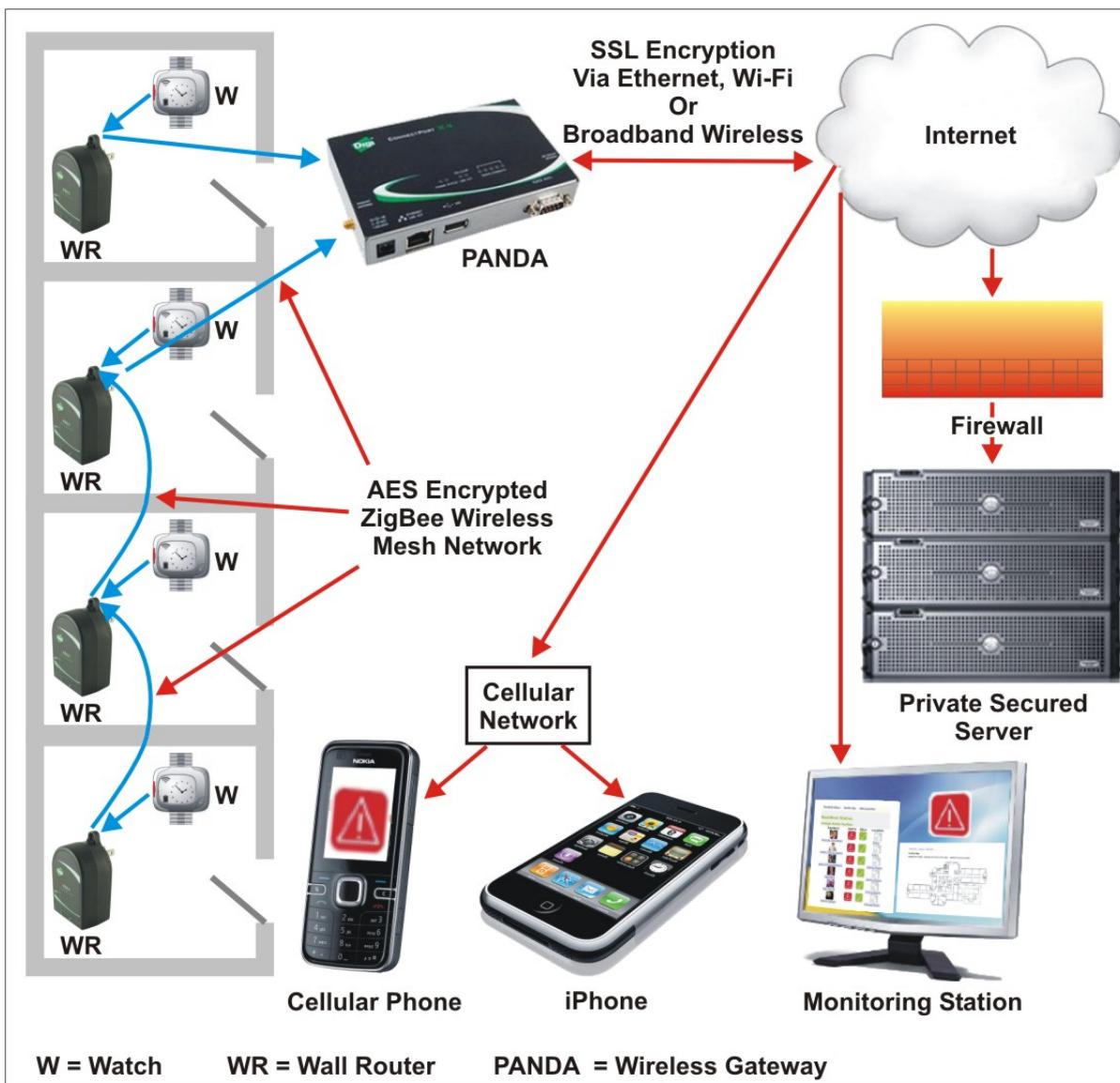

Figure 2.2 Interconnection and dataflow between several MobileCare™ Monitor components.

5

2.2 Overview of myPHD

The myPHD allows the residents to be mobile while being monitored by the network. The myPHD periodically transmits the location of the resident within the facility and clinical data to the CareStation™ software. It has two buttons:

o **Emergency** button – During an emergency, the resident presses this button to issue an emergency alert to the caregiver's station.
o **Privacy** button – The residents use this button to stop sending clinical data to the CareStation™ Software for a pre-set interval of time.

Figure 2.3 The myPHD with buttons.

Furthermore, the myPHD contains:

• **Built-in temperature sensor** – provides resident skin (body) and ambient air temperatures to help determine if the watch is being worn.

• **Impact sensor** – issues an alert when the myPHD receives an impact (such as when a resident falls).

• **Battery charge level indicator** – displays the remaining battery charge.

> *Ensure that the myPHD is positioned properly on the monitored individual's wrist.*

2.3 Components of the MobileCare™ Monitor System

Table 2.1 describes the various components and features of the MobileCare™ Monitor System:

Component	Features
XBee Wireless Wall Router	- Installed in key locations throughout the facility - Connects to other XBee routers in a secure wireless mesh network (for further information on the security of the wireless network, refer to *Chapter 4.0 Security*.) - Picks up the messages or alerts transmitted by myPHDs and forwards messages/alerts to the PANDA X4 gateway for subsequent delivery to the server - Receives (wireless) messages and alert-acknowledgements from the PANDA X4 gateway and forwards the messages/alerts to the relevant myPHD
PANDA (Powered Automated Network Data Aggregator) X4 Gateway	- Gateway between the Internet and the internal wireless mesh network - Connects to the Internet via Ethernet, Wi-Fi, or Broadband - Sends the received messages from the XBee routers to the secure server - Communicates wirelessly with the myPHDs and the central server, allowing total freedom of movement of the residents throughout the facility - Delivers email or text message alerts to various devices such as cell phones, PDAs, and MobileCare™ Monitoring Stations
Secure Server. *See Figure 2.1.*	- Sets up behind a firewall at a high availability Web Hosting data center - Maintains all resident information, including location, collected data, and alerts - Monitors the PANDA x4 gateway, the XBee routers, and the myPHDs via two-way communication and automatically raises an alert if any device malfunctions - Can be accessed by the end user over the Internet using a web browser - Can be connected directly to a DSL or Cable Modem / Router in a SOHO environment

7

Component	Features
CareStation™ Software	• Web-browser based software application • Provides an easy-to-use, yet secure, graphical user interface to allow the caregivers and administrative staff to respond to myPHD alerts • Integrates a facility map to provide resident location information to the caregivers, based on the information received from myPHDs • Provides access to the secure server so caregivers can view and analyze the resident's information • Provides actionable, clinical data as well as specific reports to improve health-care management • Assists health care staff in providing individual, personalized care

Table 2.1 MobileCare™ Monitor System Component and Features.

The operators should use only AFrame Digital specified sensors and third-party devices. AFrame cannot guarantee or be responsible for overall system functioning if non-approved sensors or devices are used.

The XBee Wireless Wall Routers are installed and serviced only by authorized AFrame Digital, Inc. representatives. Do not attempt to open or service the routers at any time.

The PANDA X4 Gateway is installed and serviced only by authorized AFrame Digital, Inc. representatives. Do not attempt to open or service the device at any time.

2.4 Compliance to Electromagnetic Compatibility Standard

The MobileCare™ Monitor System complies with International Standard EN 60601-1-2:2004 for electromagnetic compatibility (EMC) for medical electrical equipment or systems, or both. This standard is designed to provide reasonable protection against harmful interference in a typical medical installation.

8

3.0 Operating Procedures

This chapter provides instructions on how to wear and operate the myPHD, interpret the messages displayed in the panel, and trigger and send emergency alerts. This chapter explains the features of the CareStation™ Software and the procedure to respond to alerts, detect the location of residents, and view the clinical and historical data of the residents.

MyPHD is the only component of the MobileCare™ Monitor System operated by the end user (residents). Before using myPHDs, the operator must ensure the proper installation of all components of the MobileCare™ Monitor System.

> *The components of the MobileCare™ Monitor System should not be installed by the end user. These components (such as the routers, the gateway, and the server) must be installed by the representatives of AFrame Digital, Inc. who are trained in the proper installation techniques.*

3.1 Using myPHD

This section explains how to:

- Wear myPHD and use the various options.
- Check for out-of-range status.
- Send emergency alerts using myPHD.
- Analyze the messages displayed by myPHD.

> *The myPHD is the key component of the MobileCare™ Monitor System that has to be worn and operated by the residents or patients. Hence, the operators must ensure that they thoroughly understand the operating procedures of myPHD.*

3.1.1 Wearing myPHD

The myPHD alerting device resembles a watch and should be worn like a wristwatch. The watch should be worn continuously. The myPHD has built-in sensors that determine if the device is being worn. The server constantly monitors these details and raises an alert if a resident removes the myPHD from his/her wrist.

> *The myPHD alerting device should not be exposed to water.*

9

3.1.2 Installing the Batteries

The batteries in myPHD should not be installed or changed by the residents or caregivers. Only an authorized representative of AFrame Digital, Inc. will service the batteries. Batteries must be recharged after several days under normal use conditions.

3.1.3 Using myPHD Buttons

MyPHD has two buttons: **Emergency** button and **Privacy** button.

Figure 3.1: The myPHD with buttons

Table 3.1 summarizes the use of these buttons.

Press	Result
Emergency button	Send an emergency alert to the caregiver and administrative staff.
Privacy button	Temporarily stop myPHD from sending clinical data to the AFrame CareStation™ Software.

*Table 3.1 Usage of myPHD buttons*

10

3.1.4 Checking for Out-of-range Status

The myPHDs function properly only when they are within the range of the XBee wireless routers. If the resident moves out of range of the XBee routers, the myPHD will display a FAILED message and the myPHD will be unable to send information and alerts to the caregiver or administrative staff.

The signal strength indicator on the myPHD display will indicate if the resident is within range of the XBee wall routers.

Additionally, if the resident is within the range, myPHD will display the date and time.

Normal Operation signal – indicates the myPHD is within range of the wall routers.

When the resident moves out of the range of XBee wall routers, the signal strength indicator will change.

Additionally, a WATCH FAILED message will flash on the myPHD's display panel.

Out of Range signal – indicates the myPHD is out of the range of the wall routers.
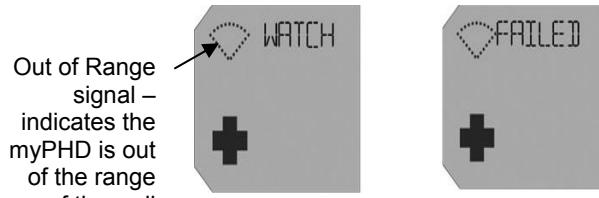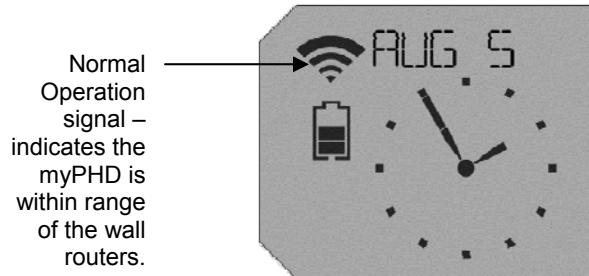
3.1.5 Verifying the Battery Charge

The charge indicator on the display panel of the myPHD will show the remaining charge of the batteries.

Indicates the battery charge level
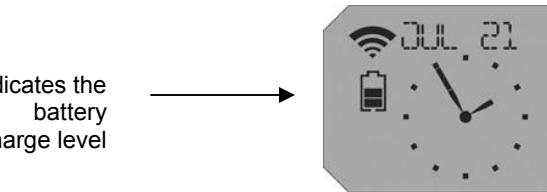
The above illustration shows the power indicator for an empty battery. In this scenario, the operator should recharge the myPHD. If it still does not function, call the support line of AFrame Digital, Inc.

11

 The myPHD alerting device, XBee wall routers, and the PANDA unit are designed to be powered ON all the time. The server constantly monitors the status of all these components and will raise an alert in the event of any failure.


3.1.6 Sending Emergency Alerts to Caregivers

When the residents or patients need the assistance of a caregiver, they can send an emergency alert using myPHD.

Before sending an emergency alert, the residents should ensure that they are within the range of an XBee wireless wall router. See *3.1.4 Checking for Out-of-range Status* for more information.

The resident should follow these instructions:

1. Press the **Emergency** button on the myPHD.
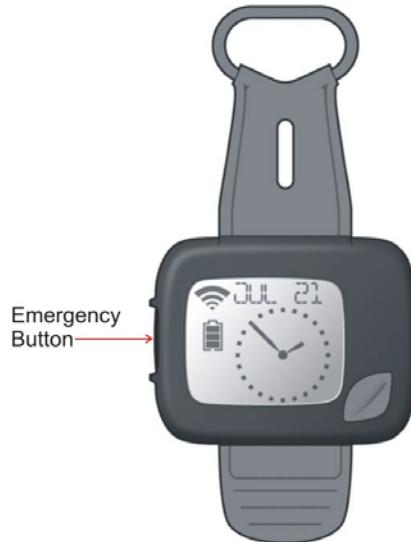
2. The date, time, and battery indicator will disappear from the screen, and the alert indicator flashes.
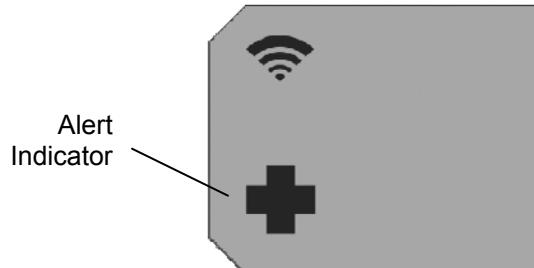
3. When the alert is transmitted
   successfully, the MSG SENT
   message will be displayed in the
   display panel of the myPHD.

4. When the administrative staff or
   caregiver acknowledges the alert
   message, the HELP COMING
   message will be displayed in the
   display panel of the myPHD.

5. Finally, the caregiver who attends to
   the call will **reset the display** back
   to normal status.
   See the section *3.1.7 Resetting
   myPHD to Normal State* for more
   information on resetting the display.

3.1.7 Temporarily Disabling Alerts

The myPHD alerting device sends resident data, location information, and alerts
using a wireless network. Sometimes, the residents may choose not to send any
data to the server or alerts to the caregiver for maintaining privacy. In such cases,
the residents can temporarily disable the myPHD from sending data for a pre-
determined number of minutes.

1. To temporarily disable the myPHD
   device from sending data, press the
   **Privacy** button.
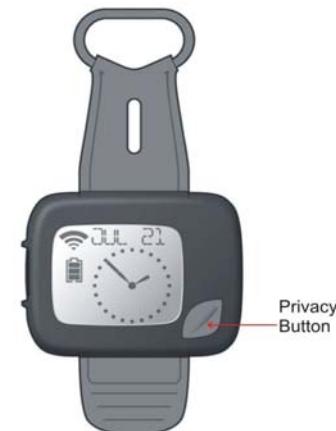
Privacy
Button

2. On the myPHD display panel:

- The **PRV** message is displayed
- The signal indicator changes to indicate no signal
- The ring around the clock changes
- The device counts down from a pre-defined number of minutes

No-signal indicator.

Countdown indicating 29 minutes of privacy remaining.

If the resident presses the **Privacy** button before the pre-defined setting time has elapsed, the privacy duration will be reset and the countdown will start afresh. In this way, the resident can extend the privacy duration, if desired.

Countdown that indicates 10 minutes of privacy period remaining.
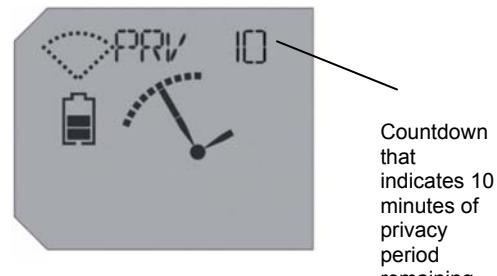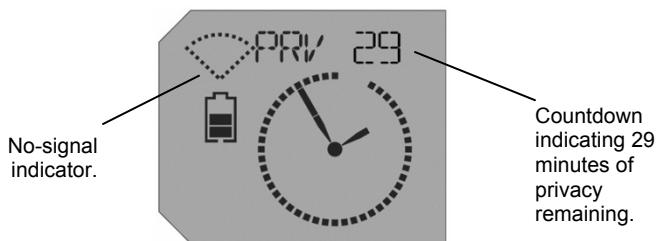
3. After the pre-defined number of minutes has elapsed, the device will switch back to normal status and once again start transmitting location and clinical data.

The privacy feature can be canceled by pressing the privacy button a second time. Pressing it a third time restarts the privacy timer.

3.1.8 Impact Sensing and Falls

The myPHD can be used in a falls reduction program to sense impacts as an indication of falls. When a resident wearing the watch falls, myPHD detects the impact and automatically sends an alert to the caregiver.

The myPHD alerting device, XBee wall routers, and the PANDA unit are designed to be powered ON all the time. The server constantly monitors the status of all these components and will raise an alert in the event of any failure.

14

3.1.9 Canceling Alerts

If the residents send emergency alerts by mistake, they can cancel the alert before it reaches the caregiver. Also, if they drop myPHD by mistake, they can cancel the emergency alert before it reaches the caregiver.


You can cancel the alert only before the MSG SENT message is displayed on the display panel.

---

1. Before the **MSG SENT** message appears on the display panel, press the **Privacy** button.

Privacy Button

2. The emergency alert will be canceled and the **EM MSG CANCLD** message will be displayed on the display panel.
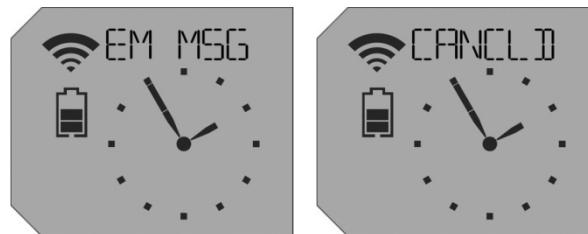
3. The myPHD device will then switch back to normal mode.

Pushing the emergency button or falling will generate an alert message overriding the privacy feature.

3.1.10 Interpreting Error Messages

Message Displayed on myPHD	Meaning and Actions to be taken
EM MSG CANCLD	Displayed when the resident cancels the emergency alert before it was sent to the caregiver.
HELP COMING	Displayed when the caregiver acknowledges the alert.
MSG SENT	Displayed when the alert message has been sent to the caregiver. The resident must wait for acknowledgment from the caregiver.
FAILED	Displayed when the resident moves away from the range of the MobileCare™ Monitor System. In such situations, instruct the residents to move within the range.
NO FNC	Displayed when the resident presses the **Privacy** button while out of the signal range of the MobileCare™ Monitor System. The resident must move inside the signal range of the MobileCare™ Monitor System.
PRIVCY	Displayed when the resident has activated the privacy mode on the myPHD device.
PRV *nn*	Displayed when the myPHD device is in privacy mode and is not sending any resident data (*nn* is the number of minutes of privacy remaining). The myPHD device will not send any data to the server for the indicated number of minutes. If the resident wants to extend the privacy period for some more time, he/she should press the **Privacy** button again.
WATCH FAILED	Displayed when the alert is not sent or if the caregiver does not acknowledge the alert. Wait till the administrative staff rectifies the error.

Table 3.2 Messages displayed in myPHD

3.2 Using the Charger

For charging the myPHD, place the myPHD watch on the charger as shown in the following photograph.

Figure 3.2.0: The myPHD is placed on the charger.

The LED on the charger (see the photograph below) indicates the status of charging.

Figure 3.2.1: The charger LEDs.

The LEDs on the charger provides three possible status scenarios, as stated in the following Table.

Rapidly Flashing Red	Failure
Blinking Green	Charger is charging the myPHD
Solid Green	Charging Complete

When the myPHD is placed on the charger, the myPHD display confirms this event as "CHARGE."

When the myPHD shows "CHARGE", it enters in to a low power sleep mode and disables its connection with the ZigBee radio.

3.3 Using the CareStation™ Software

This section explains the features of the CareStation™ Software and is relevant to caregivers and the administrative staff of the facility.

The CareStation™ Software is an easy-to-use web-browser based secure application for helping caregivers and administrative staff to respond to myPHD alerts. In addition, the operators can use the software to:

- View the location of a resident on the pre-installed facility map.

- View and analyze data collected from the residents.

- View specific reports to help improve management of the facility.

3.3.1 Logging into the CareStation™ Application

1. Open a Web browser and go to `https://pr.aframedigital.com.`

2. In the login screen (*see Figure 3.2*), enter your **User Name** and **Password**.

3. Click **Sign In**.

Figure 3.2 MobileCare™ Monitor Login Screen

The operators will be asked to change the password every 90 days. The operators should not disclose their user name or password.

4. After logging in, the operator will be able to see the main screen (Resident Status screen) of the CareStation™ application.

3.3.2 Understanding the Resident Status Interface

The Resident Status screen (*see Figure 3.3*) is the main screen that is displayed to the operators after they login to the CareStation™ application. The Resident Status screen shows the status (such as alerts or Activity of Daily Listings (ADL)) of all the residents of the facility. It also displays the last known location of the residents.

Figure 3.3 The Main Screen – Resident Status
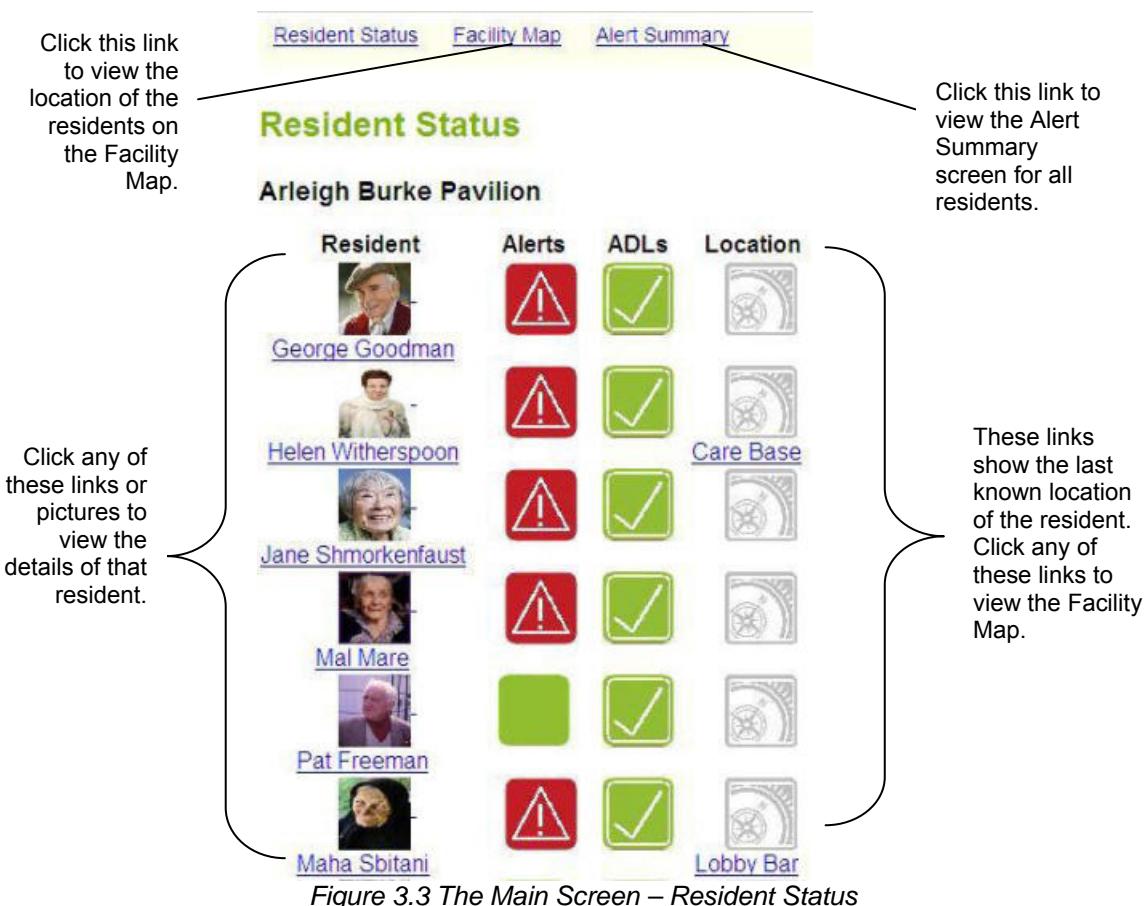
To return to the Resident Status screen from the other screens, the operator has to click the Resident Status present at the top of the screen.

The following table summarizes the available options:

Click the	To
Picture or name of a resident	View the details of that resident
Alert icon adjacent to the resident's name	View the alerts for the resident from the alert summary screen
ADL icon adjacent to the resident's name	View ADL data of a specific resident
Location icon adjacent to the resident's name	View that location in the Facility Map
Facility Map link at the top of the screen.	Open the Facility Map screen
Alert Summary link at the top of the screen.	Open the Alert Summary screen

Table 3.3 The available options

This resident status screen displays a green icon for residents whose alerts have been responded to.

3.3.3 Understanding the Resident Detail Interface

To view the details of a resident, the operator will click the name or picture of the resident. The details of the resident along with their last known location, air and skin temperature, the address to which alert was sent, notes, history of alerts, and so on are displayed (*see Figure 3.4*).

Figure 3.4 Details of a particular resident

3.3.4 Understanding the Alert Summary for a Particular Resident

To view the alert details of a particular resident (*see Figure 3.5*), the operator can click the **Alerts Summary** icon ⚠ of that resident from the Resident Status screen.

Figure 3.5 Alert summary of a particular resident

There are four types of Alarm Indicators which are based on the status of the resident alert. The following are the various alarm indicators:

- 🟩 — Acknowledged

- ⚠ — Needs Help

- F — False Alarm

- E — Escalated

3.3.5 Understanding the Alert Summary for All Residents

To view the alert details of residents (*see Figure 3.6*), the operator can click the **Alerts Summary** link displayed at the top of the Resident Status screen.

Figure 3.6 Alert details of all residents

3.3.6 Understanding the Facility Map Interface

This facility map is always integrated with the CareStation™ software

---

To locate the resident graphically within the facility, the operator clicks the Facility Map link displayed at the top of the Resident Status screen. This screen displays the last known location of each resident (*see Figure 3.7*). On the facility map, the image border is red if an alert is pending and green if alerts are not pending.
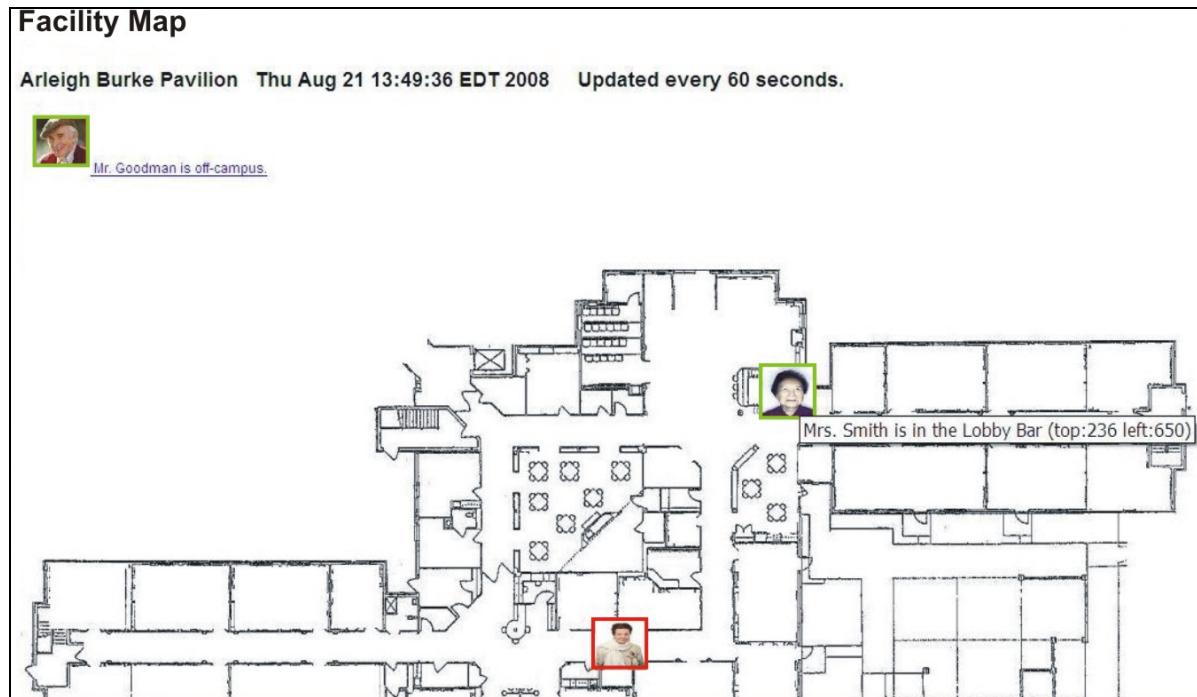
Figure 3.7 The Facility map showing the location of residents

3.3.7 Receiving and Responding to Alerts in CareStation™ Software

To respond to the alerts received from a resident, the operator clicks the particular Alert from the Resident Status screen (*see Figure 3.8 (a)*). The list of alerts from the resident is displayed in the Alert Summary screen. The operator then clicks the alert that needs attention (*see Figure 3.8 (b)*) and must be acknowledged (*see Figure 3.8 (c)*).
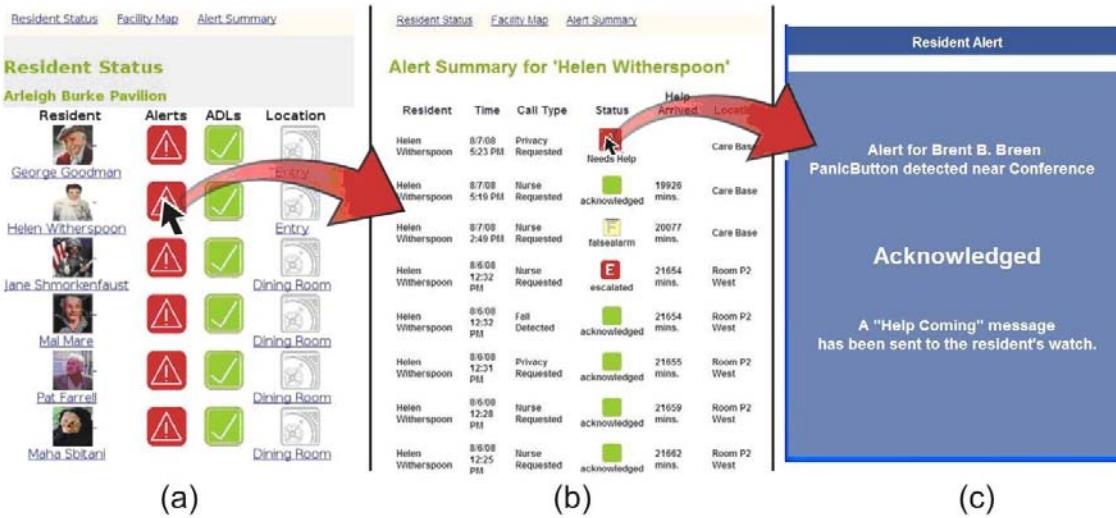
Figure 3.8 Responding to an alert

In this screen, the operators can perform any of the following operations:

- **Acknowledge** the alert, indicating assistance is on the way.

- Cancel the alarm by selecting the **False Alarm** option.

- **Escalate** the alarm to the next person (for instance, the supervisor or next-in-command) up in the line to assist.

After the operator clicks Acknowledge, the Alert Acknowledged message will be displayed on the screen and the myPHD.

3.3.8 Receiving and Responding to Alerts on Other Devices

The system administrator configures the MobileCare™ Monitor System to send the alerts to the operator's cell phone, PDA (personal digital assistant), or web-enabled phone such as iPhone.

Cellular Phone
On a cellular phone with text messaging capability, only text messages will appear. When a resident presses the emergency alert button, the system generates and sends a text message, such as the following message, to the operator's cell phone:

From: Alert System

To: myname@aframedigital.com

Sent: Wednesday, July 09, 2008 1:08 PM

Subject: Status report: Witherspoon, Helen

This is to inform you that Witherspoon, Helen has Pressed their WatchButton2Push at 1:08 PM, EDT.

https://pr.aframedigital.com/CareStation/nb/ar.jsp?nc=H4liFpP6dNTVC4JH

From text-based cellular phones, the operators cannot acknowledge the alerts.

Smart Phone or iPhone

On a smart phone or iPhone, the operator receives a text message similar to that sent to a cellular phone. However, the operator can click the link in the message to go to a graphical screen.
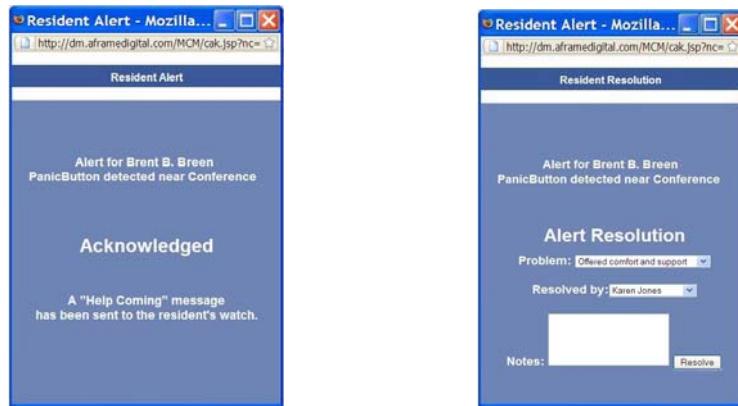
Figure 3.9 Acknowledgement and Alert Resolution Screens for a Particular Resident

After the resident has received care, the operator will resolve the alert by entering the type of problem, the name of the caregiver, and notes regarding the incident.

After the operator clicks either Acknowledge or Resolve, a message will be displayed on the CareStation™ screen and on the myPHD.
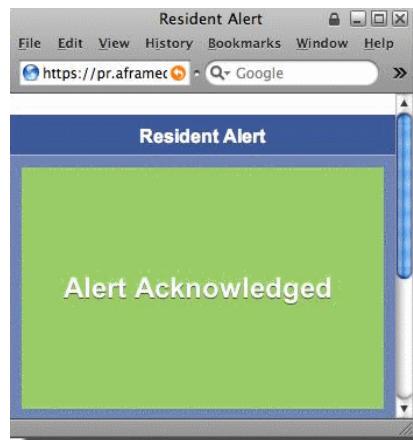
Figure 3.10 The Alert Acknowledged message

3.3.9 Clearing the Alerts

Operators can clear the alerts from the Alert Summary screen by clicking the **Needs Help** icon (*see Figure 3.6*). When clicked, a web page will be displayed that is similar to the web page displayed on the iPhone (*see Figure 3.9*) from where they can respond to the alert.

4.0 Security

The AFrame System incorporates best-practice security controls designed to protect against both anticipated and unanticipated security threats. This section provides a brief overview of the important controls.

4.1 Mesh Security

The primary threats to security on the ZigBee mesh are unauthorized access and modification of transmitted data, unauthorized devices accessing the network, and denial of service attacks against the network. The AFrame System protects against these threats using the standard ZigBee security mechanisms.

The AFrame System implements the ZigBee Standard Security Model. Unauthorized access and modification of transmitted data is prevented by encrypting all traffic between network devices including myPHD, Pandas, and ZigBee wall routers. Traffic is encrypted with the Advanced Encryption System (AES) encryption algorithm using 128-bit keys. AES is the standard symmetric encryption algorithm of the U.S. Government. AES has been analyzed extensively and is used worldwide to protect sensitive data.

To keep unauthorized devices from joining the ZigBee network, each device is authenticated using a special link key that is preconfigured on every device. When a device attempts to join the network, the PANDA uses this link key to distribute a network key which in turn is used to encrypt and decrypt traffic. If the device does not have the correct link key, it will not be allowed to join the network.

The AFrame System protects against denial of service attacks by continuous monitoring of the health and connectivity to connected devices. If an attack degrades the health of a device or of the network, it will be quickly detected and reported. Once detected, the source of an attack can be identified and neutralized.

4.2 Internet Security

The primary threats to security on the Internet are unauthorized access and modification of transmitted data, spoofing of Internet-connected components, and denial of service attacks. The design of the AFrame System uses standard Internet security mechanisms and practices to protect against these threats.

To protect against unauthorized access and modification of transmitted data, all Internet traffic is encrypted using strong Secure Socket Layer (SSL) encryption. This

includes traffic that flows between the PANDA and the AFrame Server, and traffic that flows between the Web browser used by the caregiver and the server. The AFrame System uses the same strong SSL encryption used by leading financial institutions to protect high-value financial transactions on the Internet.

A spoofing attack is an attack where a malicious entity on the Internet pretends to be a legitimate entity in order to violate security in some way. To prevent spoofing, all AFrame components carefully authenticate their peers before communicating with them. This authentication is performed as follows:

- The Panda authenticates the AFrame Server using SSL and a 1024-bit RSA public-key certificate. This is the same mechanism used to authenticate banking web sites on the Internet.

- The AFrame Server authenticates PANDAs using standard HTTP Basic Authentication. Each request from the PANDA includes a username and password that authenticates the request. If the request contains a valid username and password, then the server will accept the message from the PANDA. If there are any discrepancies in the credentials the request will be rejected. This username and password travels over the SSL authenticated and secured connection such that they are protected against disclosure.

- When caregivers access the CareStation™ application on the server, the server authenticates the user with a unique username and password. Passwords are required to meet complexity requirements to ensure that they cannot be guessed. This username and password travels over the SSL authenticated and secured connection such that they are protected against disclosure.

- The Web browser used by the caregivers authenticates the AFrame Server using the same SSL and 1024-bit RSA public-key certificate mechanism described above. The AFrame server name shown while the caregiver checks the security on the caregiver secure page provides strong assurance that the caregiver is communicating with the correct server.

After requests are authenticated using the mechanisms described above, other validations are performed to provide additional security. For example, when the server processes the message from the PANDA, it validates that the Extended Unique Identifier (EUI) presented has been registered on the server as a valid PANDA. Similarly, when a PANDA sends watch information to the server, the server validates that the EUI of the watch has been registered with the system. The message will be rejected if the EUI is not registered.

29

4.3 Server Security

The AFrame Server stores information about caregivers and residents. The primary threats to the Server are Internet-based attacks and insider threats. These threats are countered though a variety of physical, technical, and procedural controls.

To protect against Internet-based threats, the AFrame Server is protected by external and internal firewalls. The internal firewall implements a default deny security policy whereby only essential traffic is allowed to reach the system. Furthermore, the server is hardened to run only essential services. Administrative access to the server is only permitted via public-key authenticated Secure Shell (SSH) access and all administrative traffic is protected using strong encryption. To ensure that the server is not left vulnerable to attack, strict configuration and security patch management procedures are followed. As an additional measure, AFrame periodically performs security scanning to validate its security posture.

To protect against internal threats, logical and physical access to the server is strictly controlled. Server administration is performed under the principle of least privilege, whereby administrators are given the level of access required to perform their duties and no more. To ensure that administrators are accountable for their actions, the system is configured to perform detailed auditing. To ensure that the server is physically secure, the AFrame Server is hosted in a physically secure facility with 24x7x365 monitoring.

5.0 TroubleShooting

This section describes the troubleshooting procedure for both myPHD and PANDA.

5.1 Troubleshooting myPHD and Battery

For the proper working of myPHD, ensure that:
- Battery is properly charged.
- Unit is functioning.
- Alert is generated when the Nurse call button is pressed.
- Light indicators are working.

5.2 Troubleshooting PANDA

For the proper working of PANDA, ensure that:
- Power cord is plugged correctly.
- Network activity light of the Ethernet port is blinking.
- Power is ON.
- ZigBee activity light is ON.

For assistance call (703) 560-0512 or email to support@aframedigital.com.

Appendix A — Warranty

AFRAME DIGITAL, INCORPORATED (AFRAME) warrants to the purchaser, for a one year period from the date of initial purchase or service subscription each MobileCare^{TM} Monitor 2100 (MobileCare™ Monitor 2100). AFRAME shall repair or replace any MobileCare™ Monitor 2100 found to be defective in accordance with this warranty, free of charge, for which AFRAME has been notified by the purchaser by serial number that there is a defect, provided said notification occurs within the applicable warranty period. This warranty shall be the sole and exclusive remedy by the purchaser hereunder for any MobileCare™ Monitor 2100 delivered to the purchaser which is found to be defective in any manner whether such remedies be in contract, tort, or by law. This warranty excludes cost of delivery to and from AFRAME. All repaired units shall be received by the purchaser at AFRAME's place of business. For any MobileCare™ Monitor 2100 sent to AFRAME for warranty repair that is found to be within specification, the purchaser agrees to pay $100.00 (US Dollars) to defray costs of handling and testing. The MobileCare™ Monitor 2100 is a precision electronic instrument and must be repaired by knowledgeable and specifically trained AFRAME personnel only. Accordingly, any sign or evidence of opening the MobileCare™ Monitor 2100 or any of its components, field service by non-AFRAME personnel, tampering, or any kind of misuse or abuse of the MobileCare™ Monitor 2100, shall void the warranty in its entirety.

DISCLAIMER/EXCLUSIVITY OF WARRANTY:
THE EXPRESS WARRANTY SET FORTH IN THIS MANUAL IS EXLCUSIVE AND NO OTHER WARRANTY OF ANY KIND WHETHER STATUTORY, WRITTEN, ORAL, OR IMPLIED INCLUDING WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR SETTING SHALL APPLY.

The standard rates and charges in effect will be levied on all non-warranty work.

Appendix B — Service

The MobileCare™ Monitor and its components are precision electronic instruments and must be repaired only by trained AFrame representatives. Any sign or evidence of opening the system, service by non-AFrame personnel, tampering, or any kind of misuse or abuse of the system, shall void the warranty in its entirety.

For additional technical information contact AFrame's Customer Support department at:

AFrame Digital, Inc.
8000 Lee Highway
Falls Church, VA 22042
(703) 560-0512
Email: service@aframedigital.com
www.aframedigital.com

The standard rates and charges in effect will be levied on all non-warranty work.

Appendix C — Declarations

See http://www.iec.ch for the FCC and IEC standards.

Federal Communications Commission (FCC) Notice

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Refer to the following tables for specific information regarding this device's compliance with IEC 60601-1-2.

Electromagnetic Emissions

EMISSIONS TEST	COMPLIANCE	ELECTROMAGNETIC ENVIRONMENT—GUIDANCE
This device is intended for use in the electromagnetic environment specified below. The customer and/or user of this device should ensure that it is used in such an environment.		
RF Emissions CISPR 11		
RF Emissions CISPR 11		
Harmonic Emissions IEC 61000-3-2		
Voltage Fluctuations/Flicker Emissions IEC 61000-3-3		

Electromagnetic Immunity

IMMUNITY TEST	IEC 60601 TEST LEVEL	COMPLIANCE LEVEL	ELECTROMAGNETIC ENVIRONMENT— GUIDANCE
This device is intended for use in the electromagnetic environment specified below. The customer and/or user of this device should ensure that it is used in such an environment.			
Electrostatic Discharge (ESD) IEC 61000-4-2			
Electrical Fast Transient/Burst IEC 61000-4-4			
Surge IEC 61000-4-5			
Voltage dips, short interruptions, and voltage variations on power supply input lines IEC 61000-4-11			
Power Frequency (50/60 Hz) Magnetic Field IEC 61000-4-8			

NOTE: U_T is the AC mains voltage before application of the test level.

Guidance and Manufacturer's Declaration—Electromagnetic Immunity

IMMUNITY TEST	IEC 60601 TEST LEVEL	COMPLIANCE LEVEL	ELECTROMAGNETIC ENVIRONMENT—GUIDANCE
This device is intended for use in the electromagnetic environment specified below. *The customer and/or user of this device should ensure that it is used in such an environment.*			
Portable and mobile RF communications equipment should be used no closer to any part of the device, including cables, than the recommended separation distance calculated from the equation applicable to the frequency of the transmitter.			
Conducted RF IEC 61000-4-6 Radiated RF IEC 61000-4-3			

a. Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radios, amateur radio, AM and FM radio broadcast and TV broadcast cannot be predicted theoretically with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, an electromagnetic site survey should be considered. If the measured field strength in the location in which the device is used exceeds the applicable RF compliance level above, the device should be observed to verify normal operation. If abnormal performance is observed, additional measures may be necessary, such as reorienting or relocating the device.
b. Over the frequency range 150 kHz to 80 MHz, field strengths should be less than [3] V/m.

NOTES:
- At 80 MHz and 800 MHz, the higher frequency range applies.
- These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people.

Recommended Separation Distances

The following table details the recommended separation distances between portable and mobile RF communications equipment and this device.

	Separation Distance According to Frequency of Transmitter		
	This device is intended for use in an electromagnetic environment in which radiated RF disturbances are controlled. Users of this device can help prevent electromagnetic interference by maintaining a minimum distance between portable and mobile RF communication equipment (transmitters) and the device as recommended below, according to maximum output power of the communications equipment.		
Rated Maximum Output Power of Transmitter W	150 kHz to 80 MHz $d = 1.17 \sqrt{P}$	80 MHz to 800 MHz $d = 1.17 \sqrt{P}$	800 MHz to 2.5 GHz $d = 2.33 \sqrt{P}$
0.01			
0.1			
1			
10			
100			

For transmitters rated at a maximum output power not listed above, the recommended separation distance *d* in meters (m) can be estimated using the equation applicable to the frequency of the transmitter, where *P* is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer.

NOTES:
- At 80 MHz and 800 MHz, the higher frequency range applies.
- These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection from structures, objects, and people.

Appendix D — Specifications

The following are the specifications of myPHD Wireless Personal Help Watch:

myPHD Specifications

PARAMETER	SYMBOL	CONDITION	MIN	TYP	MAX	UNITS
Operating Range						
Acceleration Range	g_{FS2g}		-2		2	g
	g_{FS4g}	Switchable via serial digital interface	-4		4	g
	g_{FS8g}		-8		8	g
Supply Voltage (Analog)	V_{DD}		2.4		3.6	V
Supply Voltage for Digital I/O	V_{DDIO}	VDDIO ≤VDD	1.62		3.6	
Supply Current Normal Mode	I_{DD}	Digital and Analog		200	290	μA
Supply Current Standby Mode	I_{DDsbm}	Digital and Analog		1	2	μA
Operating Temperature	T_A		-40		+85	°C

Table 1: Operating range, output signal and mechanical specifications of the SMB380

Acceleration Output Signal						
Acceleration Output		Format			10	Bit
Resolution		2's complement				
Sensitivity	S_{2g}	g-range ±2g	246	256	266	LSB/g
	S_{4g}	g-range ±4g	122	128	134	LSB/g
	S_{8g}	g-range ±8g	61	64	67	LSB/g
Zero-g Offsett	Off	TA=25°, calibrated	-60		60	Mg
Zero-g Offsett	Off	TA=25°, over lifetime	-150		150	Mg
Zero-g Offset Temperature Drift		Over TA		1		Mg/K
Bandwidth	Bw	2nd order analog filter		1500		Hz
		Digital Filter		25, 50, 100, 190, 375, 750		Hz
Acceleration Data Refresh Rate (all axes)	f_rate		2700	3000	3300	Hz

PARAMETER	SYMBOL	CONDITION	MIN	TYP	MAX	UNITS
Nonlinearity	NL	Best fit straight line	-0.6		0.5	%FS
Output Noise	n_{rms}	Rms		0.5		Mg/√Hz
Sensitivity	S_T	Preliminary data	0.475	0.5	.0.525	K/LSB
Temperature measurement range	T_S		-30		97.5	+/- .5° C
Temperature Offset	Off_T	Calibrated at 30°C		1		K
Mechanical Characteristics						
Cross Axis Sensitivity	S	Relative contribution between 3 axes			2	
Mechanical Shock		Duration ≤ 100μs			10,000	G
		Duration ≤ 1.0ms			2,000	G
		Free fall onto hard surface			1.5	M
ESD		HBM, at any pin			2	kV
		CDM			500	V

Specifications are subject to change without notice. Please contact AFrame Digital, Inc. for current specifications.

PANDA X4 Gateway Specifications

Network protocols	• UDP/TCP, DHCP.
LEDs	• ConnectPort X4: Ethernet status, power, cellular link/activity, signal strength (4 bars), ZigBee link/activity, Wi-Fi link/activity.
Security – ConnectPort X4	• Security – SSL tunnels, SSHv2, FIPS 197 (serial port). • Real-time clock.
Router/Security Features	• NAT. • Port forwarding. • Access control lists (IP filtering).
VPN Features – ConnectPort X4	• IPsec with IKE/ISAKMP. • Multiple tunnel support. • DES, 3DES and up to 256-bit AES Encryption. • VPN pass-through, GRE forwarding.
Management	• HTTP/HTTPS web interface. • Password access control. • IP service port control. • Optional secure enterprise management via Digi Connectware Manager.

Interfaces	• **Serial – ConnectPort X4**
	  o 1 RS-232 DB-9M serial port.
	  o Throughput up to 230 Kbps.
	  o Full signal support for TXD, RXD, RTS, CTS, DTR, DSR and DCD.
	  o Hardware and software flow control.
	• **USB**
	  o ConnectPort X4: 1 Powered USB Type A connector (Host). See www.digi.com/products/wireless/usb-peripherals/ for the list of supported USB devices.
	• **Ethernet**
	  o 1 RJ-45 port
	  o Standard: IEEE 802.3
	  o Physical Layer: 10/100Base-T
	  o Data rate: 10/100 Mbps (auto-sensing)
	  o Mode: full or half duplex (auto-sensing)
	• **ZigBee/802.15.4**
	  o XBee-PRO (Freescale and Ember supported).
	  o Cellular.
	  o ConnectPort X4: EV-DO/1xRTT or EDGE/GPRS PCI Express Module (1).
	  o Wi-Fi (802.11b) – ConnectPort X4.
	  o Standard IEEE 802.11b.
	    ▪ Frequency: 2.4 GHz.
	    ▪ Data rate: Up to 11 Mbps w/ fallback.
	    ▪ Modulation: DBPSK (1 Mbps), DQPSK (2 Mbps), CCK (11, 5.5 Mbps).
	    ▪ Transmit power: 16 dBm typical.
	    ▪ Receiver sensitivity: –82 dBm @ 11 Mbps.

	▪ Connector: 1 x RP-SMA.0 ▪ Ad-hoc & AP Client Modes only; Access Point Mode not supported. ▪ Not available when gateway is configured with a cellular module.

Environmental Specifications	• Operating temperature:
	  o ConnectPort X4 (CDMA models): –30° C to 60° C (–22° F to 140° F)
	• Relative humidity: 5% to 95% (non-condensing)
	• Ethernet isolation: 1500VAC min per IEEE802.3/ANSI X3.263
	• Serial port protection (ESD) – ConnectPort X4, X8
	  o +15 kV Air Gap and +8 kV contact discharge per IEC 1000-4-2

Regulatory Approvals	• ConnectPort X4:
	  o Safety: UL 60950, CSA 22.2 No. 60950, EN60950
	  o Emissions/Immunity: CE, FCC Part 15 (Class A), AS/NZS CISPR 22, EN55024, EN55022, Class A
	  o Mobile Certifications – CDMA/EV-DO: CDG, TIA/EIA-690, TIA/EIA-98-E
	  o Mobile Certifications – GSM/UMTS: PTCRB, NAPRD.03, GCF-CC, R&TTE, EN 301 511

Power Requirements	• Power input
	  o ConnectPort X4: 6-30VDC
	  o 12V DC power supply for 0° C to 60° C (32° F to 140° F) with locking barrel connector included; extended temperature power supply available separately
	• Power consumption
	  o ConnectPort X4: Idle: 1.5 W, Max: 10.4 W
	• Surge protection (with included power supply): 4 kV burst (EFT) per-4-4, 2 kV surge per EN61000-4

Dimensions	• ConnectPort X4
	  o Width: 3.35 in (8.50 cm)
	  o Height: 1.00 in (2.54 cm)
	  o Length: 5.25 in (13.33 cm)
	  o Weight: 2.60 lb (1.18 kg)

Antennas	• Antenna Type
	  o ZigBee/802.15.4 – 4" dipole with 2" cable, tabletop mountable (same type antenna is used for Wi-Fi configured gateways)
	  o Cellular – 7" dipole
	• Connector Type (on Gateway)
	  o 50 ohm SMA
	  o Female for ZigBee & Wi-Fi
	  o Male for cellular

Specifications are subject to change without notice. Please contact AFrame Digital, Inc. for current specifications.