Until a few years ago, health care alarms were typically localized. They either emanated from the medical device itself or, in the case of physiologic monitors, came from both the monitor and its central station. Can the use of middleware change how alarms are sent out and managed? Will it be able to create a personal notification environment for clinicians that is as simple to use as texting?

Middleware has been described as software that allows for communication and data management between two different systems. Used especially in IT networks, middleware provides messaging services so that different applications can communicate – it tries to glue everything together. While middleware can also facilitate the automation of clinical documentation, perform remote surveillance, and perform data aggregation for retrospective review and analysis, the information below focuses on how its use can revolutionize alarm management.

**ALARM MANAGEMENT AND NOTIFICATION**

In 2013, the Joint Commission (TJC) published a Sentinel Event Alert citing 98 reports of alarm-related events over a 3.5-year period, with 80 of those events resulting in deaths and 12 in permanent loss of functions. TJC then issued the 2014 National Patient Safety Goal (NPSG) for hospitals and critical-access hospitals. The NPSG focuses on managing alarms more effectively to reduce alarm fatigue and is to be implemented in two phases:

- **Phase 1:** During 2014, health care providers were required to identify the alarm hazards that organizations will address based on their individual situations.
- **Phase 2:** As of January 1, 2016, organizations will be expected to have developed and implemented specific policies and procedures to combat hazards and educate staff.

Alarm management is very complex, and making the most of emerging technologies like middleware may be a critical part of how your hospital responds to the NPSG. A middleware solution can help organizations collect alarms and data for analysis and in turn help them recognize problematic alarms.

**SYSTEM DESIGN**

Using PCDs to manage alarms can turn the complex alerting process into a simple one – or at least a less complex one. Alerts and alarms from different applications and medical devices may be routed to the middleware. The middleware can relay the alarms to the communication system that then propagates the messages to PCDs carried by medical personnel. Voice-over IP (VoIP) phones, Wi-Fi phones, smartphones, and pagers can now receive alarms that were once limited and localized. With the advance in technology, these PCDs can now also receive specific information related to the alarm device or alerts from different sources, which can lead to better alarm management.

**MIDDLEWARE’S CRITICAL FUNCTIONS**

Middleware performs critical functions, such as:

- Prioritization of alarms
- Assignments (staff assignments, schedules)
- Alarm escalations
- Routing assignments
  - Individual: the system sends the message to an individual only
  - Group: an alarm condition, such as a code blue, is set to propagate to a team
- Report generation and information logs
- Complex event processing: combines messages from multiple sources to infer
events or patterns that suggest more complicated circumstances

Properly implemented, these systems can expedite alarm notification and response times, improve alarm management, reduce alarm fatigue, and create a quieter healing environment for patients by directly notifying clinicians or caregivers via PCD and sending multiple alerts to a PCD from different alarm sources.

Of the many critical functions the middleware performs within an alarm management system, the following require great attention:

- **Prioritization**: The alarm management system must have a built-in prioritization capability. More than one alarm may emanate from a single device, and guidelines must clearly state which alert takes precedence. Accurate mapping of priorities is necessary for the system to work effectively.

- **Escalation**: Alarm escalation schemes are critical to the successful implementation of an effective system. It is essential to narrow down which alarms and alerts are to be transmitted via the middleware to the PCD. Proper implementation of an alerts system takes into account how alarms are escalated and to whom they are sent. Failover redundancies should be built in, and alarms should automatically be escalated within a certain time frame if the primary caregiver does not acknowledge an alarm.

- **Reporting**: Reducing the number of problematic alarms requires robust alarm management strategies and data analysis. Alarm systems using middleware are built to collect just that type of data. They can create reports specific to a particular care unit, to an individual device, or even based on a particular alarm priority level. This ability is vital, as it allows organizations to parse their data to find problematic alarm areas. This level of reporting can also arm an organization with audit trails to track alert delivery and response times. Alarm reports generated through a system’s middleware help educate a facility’s staff and helps them understand how to customize the type of alarms they receive.

- **Managing assignments**: Using middleware in your alarm management system allows staff to create appropriate correlations between caregivers and their assigned patients, between caregivers and their PCD, and between caregivers and their backup “buddy,” which can include other members of their group who can provide coverage, the Code Blue Team, and others.

Working with your middleware vendor and your alarm consultant is important to discuss the types of care models that are already established in your organization. Nursing care delivery models like centralized monitoring, decentralized monitoring, or a hybrid of the two will affect your choice of how your system is designed and what middleware is required.

Alarm middleware is highly complex and very customizable. Because the cost of these systems depend on their configurations, it's not uncommon for a hospital to spend more than $100,000 to implement them. To make sure you are getting the right system for your hospitals and their nursing care delivery models, it’s imperative to have a good design team in place. A good multidisciplinary team should include not only members of the clinical staff, but also IT, facilities, and biomedical engineering.

One of the biggest considerations the team must focus on is testing the middleware alarm management system. It is imperative to exhaustively analyze the system to ensure that alarms are transmitted and received properly. A “sandbox” testing environment should be set up to evaluate how well the escalation scheme functions when priority level alarms are sent. A testing environment can help identify potential glitches during software and hardware upgrades. Alarm integration is one technology in which performance improvements can be great – or devastating. Deep analysis, planning, and testing are essential to success.

**THIS ARTICLE IS EXCERPTED FROM ECRI Institute’s 2015 Top 10 Hospital C-Suite Watch List**, which includes more information on what to do to meet the National Patient Safety Goal. Download the watch list for free at www.ecri.org/2015watchlist. Want to know more about middleware vendors? Purchase the recording of ECRI’s middleware vendor webinar at www.ecri.org/middleware. To learn more, visit www.ecri.org; call (610) 825-6000; or e-mail communications@ecri.org.