A Salute to Mary Logan
Retiring President of AAMI

In this issue

PATIENT MONITORS
- A segment poised for growth and innovation p. 60

DEFIBRILLATORS
- Advancements are fueling the market p. 70

TESTING EQUIPMENT
- Innovation improves hospital efficiency p. 78
Data Management

The need to leverage enterprise medical device integration

By John Zaleski

Despite myriad public and private guidelines, reforms and standardization initiatives, many medical devices still require that their proprietary semantics and messaging format be translated to something more standardized to health IT systems.

For the foreseeable future, medical device data system (MDDS) middleware will continue to be necessary to pull data from certain classes of medical devices using vendors’ specifications, then translate and communicate it to a system of record.

The breadth and scope of MDDS middleware’s capabilities facilitates ways in which hospitals, health systems and other provider organizations can uncover means to leverage the data that flows from a device into a system of record. The use of the data to improve patient care management and clinical decision making comes immediately to mind — but that only scratches the surface of what is possible.

Critical distinctions in middleware will define how that data can be used.

While the capabilities of different middleware products overlap, there are key aspects of note for any enterprise deploying MDDS middleware to capture medical device data for operational charting and research.

Minimally, MDDS middleware needs to be able to retrieve episodic data from a medical device and translate it to a standard format. Additionally, middleware should be able to retrieve data at variable speeds to meet the requirements of various clinical operational settings. For example, clinical charting intervals normally vary based on clinical requirements from 30 seconds up to several hours.

The ability to retrieve data at variable rates, including at the sub-seconds level, requires technical capability on the part of the middleware vendor; but it also requires regulatory capabilities in the form of FDA clearances, which indicates that the middleware has mitigated the risks associated with communicating higher frequency data for alarms and analysis — even patient monitoring and intervention.

In the health IT space, FDA 510(k) clearance governs medical device connectivity and communication to medical device data systems. One of the distinctions between medical device data systems that are intended for the use of charting and active monitoring is that those systems cleared for active monitoring have demonstrated the capability to reliably communicate data and alarms that are required for patient assessment and intervention.

The ability to extract data and translate it to a system of record is part of what the FDA considers to be a medical device data system (MDDS). The FDA requires that MDDS solutions carry an FDA Class I status for general documentation. Other aspects, such as alarms and active patient monitoring, are beyond the scope (transfer, storage, conversion and display) of standard MDDS capabilities. According to the rule, if an MDDS is used beyond its intended use, this shifts the burden for oversight and compliance onto hospitals that will subsequently be classified as a manufacturer.

A Class II clearance can be achieved by a middleware vendor that demonstrates from a risk perspective that it has successfully mitigated the hazards of the data for use in live interventions, which would be consistent with alarm communication or creation of new data from raw data collected from medical devices.

For a middleware vendor to claim clearance for active patient monitoring, it must have all the checks and balances in place to ensure the receipt and delivery of all active patient data for intervention purposes from end to end — from collection point (medical device) to delivery point (the clinician). Again, the ability to deliver on the timing and receipt of data necessary for interventions and active patient monitoring is an important distinction.

Universal medical device standards won’t happen overnight, though it has been interesting to note manufacturers’ slow migration to a more standardized approach. Logistics and practicality rule the day in a world with steep costs in investment, development, acquisition and regulation. This reinforces the need to have a comprehensive and forward-looking approach to selecting an MDI and middleware provider that can support the technical and clinical needs of your health care organization.

About the author: John Zaleski, Ph.D., CPHIMS, is executive vice president and chief informatics officer of Bernoulli, a leader in real-time connected health care. Dr. Zaleski brings more than 25 years of experience in researching and ushering to market devices and products to improve health care. He received his Ph.D. from the University of Pennsylvania, with a dissertation that describes a novel approach for modeling and prediction of post-operative respiratory behavior in post-surgical cardiac patients. Dr. Zaleski has a particular expertise in designing, developing and implementing clinical and non-clinical point-of-care applications for hospital enterprises. Dr. Zaleski is the named inventor or co-inventor on seven issued patents related to medical device interoperability.

Share this story: dotmed.com/news/30437
Why it’s time for an immediate hospital alarm intervention

By Joanne Venella

In any hospital, clinical alarms have two basic purposes: to alert caregivers that intervention is required because a patient’s medical condition is deteriorating, or to remind caregivers that care needs to be delivered. Given the number of alarms and the decibel level on some units, it would be completely understandable to assume that most acute care staff operate in a constant state of emergency.

The truth is that the overwhelming majority of alarms endured by nurses, respiratory therapists and other caregivers have nothing to do with a patient’s medical condition. However, the fatigue and desensitization that results from caregivers responding to hundreds—or even thousands—of alarms every day is a clear and documented threat to patient safety.

In fact, the problem is so severe that the ECRI Institute has placed the lack of clinical alarm management among its Top 10 Health Technology Hazards several years running. In 2013, the Joint Commission made clinical alarm management a priority with its 2013 National Patient Safety Goal (NPSG:06.01.01), mandating that hospitals take definitive steps to implement policies and procedures to safely reduce and prioritize clinical alarms.

Technology can help get alarms under control—but it is not enough. Clinical and IT leadership, including nurses, respiratory therapists, biomedical engineers and information technology staff, must come together to develop the policies and standards necessary to bring meaning and action back to clinical alarms.

One of the major challenges in alarm management is separating clinically relevant alarms from non-actionable alarms (i.e., a sensor on a patient detached momentarily). However, the number of alarm-enabled medical devices on the market today, narrow alarm limits and inaccurate default settings can make alarm management a complex endeavor.

Addressing clinical alarm hazards in all their forms requires a holistic approach, free of the well-known departmental and data silos that hinder patient care and optimal clinical workflows. Technology certainly plays a critical role in alarm reduction and prioritization, but enterprise alarm management is a classic example of interdisciplinary leadership, involving clinical, IT, biomedical engineering and other departments. Alarm management is also much more than simply reducing non-actionable alarms. It’s a gateway for more seamless care and a way for hospitals to leverage hard data to make continuous improvements to their care and response processes.

**Going beyond alarm reduction**
Reducing the volume of clinical alarms sounding daily may be the primary benefit of clinical alarm management, but it is far from the only one. The process undertaken by the Hospital for Special Care (HSC), located in New Britain and Hartford, Conn., saw a dramatic reduction in the number of non-actionable alarms (80 percent), but it also enabled the hospitals to collect and distribute real-time data from 100-plus ventilators (each with its own set of alarms) and pulse oximeters for enhanced, continuous patient surveillance, and leverage data to assess caregiver responses to patient incidents.

For example, prior to implementing its platform, HSC depended on individual recollections from clinical responders after an alarm incident. Today, HSC has a clearer picture of every event. HSC can use the data provided by its platform to sort out the story behind any incident, increasing accuracy on occurrence reporting and resolution.

In addition, alarm data is used in reporting to HSC’s Performance Management Audit Committee, which monitors ventilator management performance and helps identify potential areas of improvement. HSC has also enjoyed greater automation in processes that used to be done manually, such as ventilator checks, which frees up respiratory therapists to focus more on the patient rather than the ventilator.

**About the author:** Joanne Venella is chief nursing officer at Bernoulli, and has spent her career transforming nursing care and improving processes. In combination with her Doctor of Nursing Practice degree, Venella brings both day-to-day operational experience and classroom theory to Bernoulli clients. Her areas of expertise include adult and pediatric emergency nursing, organizational throughput, patient flow and efficiency, process improvement, change management, departmental designs, redesigns, and physical plant layouts.

Share this story: dotmed.com/news/50445