FROST & SULLIVAN

A Virtual Think Tank Executive Summary

Best Practices for Managing Patient Monitoring Networks across the IT and Biomedical Departments

Frost & Sullivan, a leader in growth, innovation and leadership for more than 50 years, recently assembled a select group of biomedical engineering executives from diverse hospitals to participate in a forum on best practices for the proactive management of patient monitoring networks. More U.S. hospitals are responding to the influx of connected medical devices by reorganizing legacy patient care networks and traditional IT and Biomed departments, placing clinical engineers and IT specialists under the same department. These hospitals recognize that reliable medical device networks require Biomedical and IT departments that work effectively together to leverage digital tools that proactively scan the network for anomalies. Medical device networks are large, more complicated and more mission critical today than they have ever been. Supported by ongoing communication, clear departmental responsibilities, and a regular preventive maintenance schedule, more hospitals are layering digital monitoring solutions on top of their overall network maintenance strategy. With these changing dynamics in mind, Frost & Sullivan sought to better understand what best practices successful hospitals were taking to keep these critical pieces of infrastructure functional and supporting patient care.

PANEL PROFILE

Five panelists were Biomedical managers in U.S. hospitals. A professional with GE Healthcare's Digital Services organization was also on the panel to lend insights into how healthcare providers have been using digital solutions to keep their medical device networks operating at peak performance. Half of the Biomedical panelists were with large (>300 beds) stand-alone hospitals and half were part of health systems. All respondents reported that maintaining a patient monitoring network was extremely important, but were experiencing serious medical device network glitches and failures on a monthly basis. Some of the challenges these professionals faced in keeping their networks operational were due to the complexity of shared responsibilities in supporting those networks between the IT and Biomedical departments. When polled, half of the panelists reported the Biomedical department was responsible for maintaining medical device networks, a quarter reported it was the IT department's job and the remainder indicated other entities were responsible.

MODERATOR

- **Charlie Whelan**
  Vice President of Consulting
  Transformational Health
  Frost & Sullivan

PANELISTS

- **Laura Groselle**
  Manager, Clinical Engineering
  Cleveland Clinic

- **Richard Straub**
  Director, Clinical Engineering
  Biomed Services
  UPMC

- **Christopher George**
  Biomedical Engineering
  Supervisor
  Lancaster General Hospital

- **Ricardo Ortiz**
  Biomed Manager
  United Regional Medical Center

- **Tony Alongi**
  System Director of Clinical Engineering
  Rochester General Hospital

- **Lou Kowatch**
  Senior Director of
  Healthcare Digital Services
  GE

RELIABLE NETWORK CONNECTIVITY IS CRITICAL FOR OPERATIONAL SUCCESS

Panelists all agreed that network connectivity is a critical measure of their facilities' IT infrastructure and necessary to patient care. Clinicians and patients rely on remote patient monitoring devices to give and receive care. This dependency on information makes the network one of the most important pieces of health IT infrastructure. Consistent network functionality allows providers to interact with clinical information faster, thereby expediting patient care. As organizations continue upgrading their clinical networks and introducing a greater number of medical devices to their digital environments, managing clinical networks will become increasingly complex. The growing demand for hospital-based medical device connectivity solutions is expected to result in phenomenal changes across the continuum of care. Medical devices, such as patient monitors, infusion pumps, dialysis machines, point-of-care diagnostic devices and medical imaging systems are now routinely connected. Facilities are finding that harnessing their device data can provide significant improvements in driving patient safety and operational efficiency.

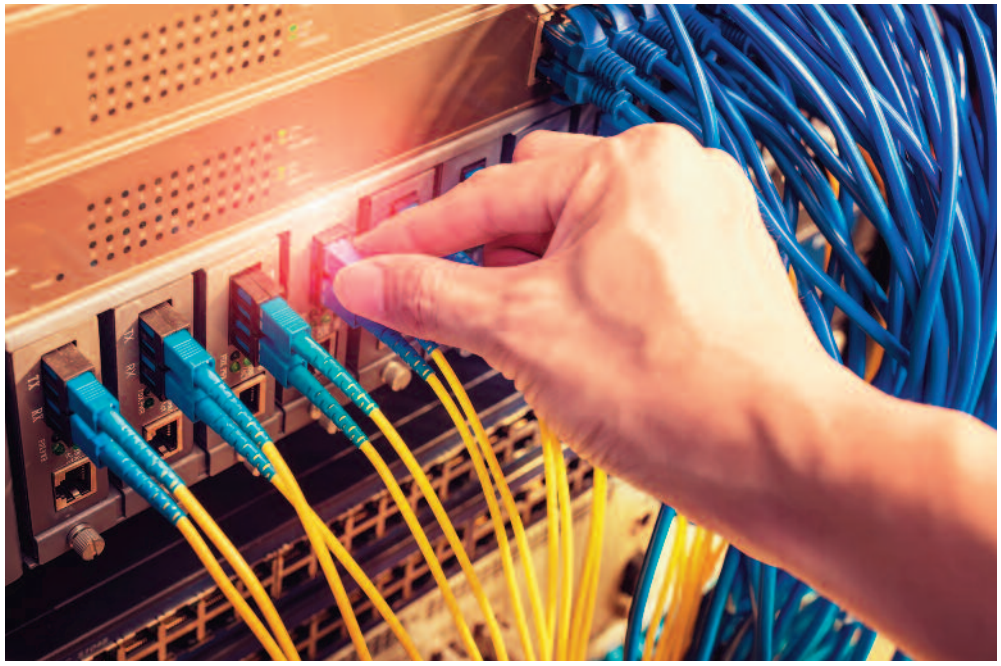
"A lot of times, network failures are caused when somebody goes into a telecommunications closet and inadvertently touches a cable or a fiber link. We've had people have power strips with switches on them, and they just brush up against them and the network goes dark. People may inadvertently turn off the power to the switches or the rack. So, a lot of things that cause network failures are just physical issues."

— Lou Kowatch,
Senior Director of Healthcare Digital Services,
GE

"This practice has helped address connectivity risks that could happen at the floor level due to actions by clinical staff. "We worked with our nursing team to improve their training and their workflows to mitigate any risk of medical device network failures."

— Tony Alongi,
Clinical Engineering Director
Rochester General Hospital

NETWORK FAILURES ARE MORE THAN AN INCONVENIENCE WHEN PATIENT SAFETY AND OUTCOMES ARE ON THE LINE



Despite knowing the advantages of maintaining reliable medical device networks, providers may not fully understand how critical proper network connectivity is to their operations. Network connectivity is essential to patient care and failures may put a patient at risk. In 2011, 2017 and 2018, the ECRI Institute identified failures in medical device and other IT networks were among the top ten health technology hazards. The organization emphasized that improved interdepartmental communication and adoption of best practices for networking medical devices were among the most effective strategies for reducing the risk of data loss or compromised safety.

> *"Inattention to best practices for implementing networked medical devices and information systems can lead to incorrect or incomplete data transfers and other data communication errors. Such errors can delay diagnosis or treatment or prompt a misdiagnosis, affecting patient safety." – ECRI Institute, 2018 Top 10 Health Technology Hazards (#9 Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care)*

COMMON CAUSES OF NETWORK FAILURES

Hospital facilities built prior to the advent of wireless communication present specific challenges to organizations looking to create modern medical device networks. Features in older buildings can block critical signals or may lack the necessary space to include the hardware required to maintain complex network infrastructure. Power outages were cited by panelists as a common reason for device networks crashing. One panelist described encountering a challenge at his hospital,"One thing that we didn't have room for originally was uninterruptible power supplies (UPSs). Not everything in our closets are in UPSs, so now I'm trying to remedy that by finding a way to get them installed on the racks or on the floor where it's needed."

Another common cause for network failures that was identified by the group was related to physical interferences in the server rooms. Lou Kowatch, Senior Director of Healthcare Digital Services with GE, indicated another common culprit for network failures is physical interference with cables and power switches."A lot of times, network failures are caused when somebody goes into a telecommunications closet and inadvertently touches a cable or a fiber link. We've had people have power strips with switches on them, and they just brush up against them and the network goes dark. People may inadvertently turn off the power to the switches or the rack. So, a lot of things that cause network failures are just physical issues."

> "One thing that we didn't have room for originally was uninterruptible power supplies (UPSs). Not everything in our closets are in UPSs, so now I'm trying to remedy that by finding a way to get them installed on the racks or on the floor where it's needed."
>
> **— A Virtual Think Tank Participant**

"Failures are sometimes due to simple things, like an IT department upgrading switches or performing patches that take down the network for the monitoring equipment. So it is essential to have a really tight relationship between IT and Biomedical where it is second nature to update each other. These are not just standard IT networks that you can patch if there's a problem"

— Lou Kowatch,
Senior Director of Healthcare Digital Services
GE

FOSTERING COMMUNICATION AND PARTNERSHIP BETWEEN DEPARTMENTS

Breaking down silos between the Biomedical and IT departments is a critical step in reducing the risk of patient monitoring network outages, as well as laying a foundation for a more effective response to dealing with those emergencies when they occur. Hospitals are using many approaches to improving that relationship. One of the most obvious yet critical strategies is developing a protocol outlining the respective responsibilities that each department has in support of the network, as well as which department is expected to act under certain types of network failures.

"Failures are sometimes due to simple things, like an IT department upgrading switches or performing patches that take down the network for the monitoring equipment. So it is essential to have a really tight relationship between IT and Biomedical where it is second nature to update each other. These are not just standard IT networks that you can patch if there's a problem," according to Kowatch.

Some hospitals are wisely taking steps to determine, in advance, the assigned responsibilities and protocols for what to do when a network goes down. Other facilities have created telephone hotlines to route questions to either Biomed or IT depending on what problem is specifically identified in order to help staff "self-triage" a network outage.

Frost & Sullivan estimates that approximately 35% - 40% of hospitals have aligned their clinical engineering department under the IT department in the facility's reporting structure. Consolidating the two departments under a single executive is one way to help reduce "turf war" conflict, but shared leadership and incentives are not a substitute for communication and planning. Other providers are using shared digital platforms and benchmarking tools that can report on network status in real time while also identifying risks when they occur. Along with using a shared data tool, these responsible parties are improving communication through regular update meetings, joint planning processes and shared project manager resources. Laura Groselle, Clinical Engineering Manager with the Cleveland Clinic,states that weekly meetings with the IT department are crucial to successful network transitions. "We rely heavily on those [weekly meetings with project managers] to keep on track."

In addition to improving the working relationships between IT and Biomedical, both departments must take steps to better integrate themselves with nursing, facilities management, central supply, finance and other departments. Rochester General Hospital's Clinical Engineering Director, Tony Alongi, says this practice has helped address connectivity risks that could happen at the floor level due to actions by clinical staff. "We worked with our nursing team to improve their training and their workflows to mitigate any risk of medical device network failures."

ADOPTING A PROACTIVE STANCE TOWARD MEDICAL DEVICE NETWORK MANAGEMENT

Hospitals are taking steps to design their networks from the ground up with features that can help reduce risk of failures. Some facilities segregate their networks to separate traffic on their existing infrastructure to enhance security and performance. Redundancy is also a critical component of logical connectivity according to Chris George with Lancaster General Hospital. "Over the years we've built a lot of redundancy so that we minimize downtime." A process he says, "built not entirely [on] trial and error" but that does help prevent similar failures in the future. As hospitals adopt more stringent ISO standards for IT network management, biomedical leaders, like George, see great value in using software tools and services that not only protect their patient data, but also ensure continuous connectivity. Even in facilities where Biomed and IT have a great relationship, there is value in using software tools and services that can be an extra check on the network in case of emergencies or simply to free up time. "Along with our internal dashboard, we use GE CNMA (Clinical Network Management Application) or their OnWatch application to proactively monitor our network. It shows us the health of the system and sends email alerts. For example, if the closet is getting too hot and the temperature exceeds the threshold of the switch, it will send us alerts."

> "Over the years we've built a lot of redundancy so that we minimize downtime."
>
> — **Chris George,** *Senior Biomedical Engineering Supervisor,* Lancaster General Hospital

> "Along with our internal dashboard, GE CNMA or their OnWatch application to proactively monitor our network. It shows us the health of the system and sends email alerts. For example, if the closet is getting too hot and the temperature exceeds the threshold of the switch, it will send us alerts."
>
> **— Chris George,**
> *Biomedical Engineering Supervisor*
> Lancaster General Hospital

More and more providers are using these types of software solutions to proactively scan and monitor their network for anomalies that can be problematic, to address issues that arise and help avoid downtime. Even for the most efficient and effective Biomedical department, using tools like these can help pinpoint network failures, saving troubleshooting time for faster problem resolutions. These solutions can also help to ensure the latest network configurations can be uploaded quickly during switch replacements. Biomedical teams are also seeing value by using these systems to monitor their UPSs and alert clinical engineers to replace batteries in order to avoid the loss of data during a power failure. The solutions can also track closet temperatures to prevent heat-related system failures.

GE's Kowatch reminded panelists that annual preventative maintenance (PM) checks are always recommended regardless of whether monitoring software is used since equipment gets dirty over time and mechanical problems, such as broken fans, can lead to components overheating. Biomedical departments are responsible for routine inspection, testing and maintenance of all medical equipment, and that includes patient monitoring networks. Chris George's strategy for ancillary devices is carried out by his internal staff. Other participants, such as Richard Straub who oversees the Clinical Engineering department at the University of Pittsburgh Medical Center, prefers to outsource some of these activities to his network providers like G.E. Regardless of how they are done, PMs are an essential part of network management.

CONCLUSION

Biomedical department managers agree that planning and communication are critical to maintaining medical device network uptime. But hospitals with even the most well-intentioned IT and Biomedical departments find it challenging to remain in constant dialogue related to any changes that one side does without the other's knowledge, which could impact the safety and security of the patient monitoring network. Software solutions that can help to proactively monitor these growing and increasingly complex networks should be part of every facility's strategy for reducing the impact of outages and data loss. These types of solutions are not a replacement for strong communication and relationships or regular preventive maintenance, but they help to reduce the risk of critical failures to patient monitoring networks that can cripple a hospital's operations.

NEXT STEPS

For more information about GE Healthcare's Clinical Networking Solutions: www.gehealthcare.com/clinicalsolutions