Lenovo
Health

IoT in Healthcare

Designing, Deploying, and Managing Integrated Io(M)T Solutions

Smarter
technology
for all

In 2020, some 30.7 billion IoT devices are expected to be active in the world. An estimated 40% of IoT devices will be used in healthcare.[1]

Yet connected health represents only 30.3% of connected devices, according to Intel.®[2]

What accounts for the difference? Unlike other industries leading the adoption of IoT, such as manufacturing, retailing, and AE&C (architecture, engineering, and construction), healthcare systems and hospitals embrace two categories of connected devices: IoT (Internet of Things) and IoMT (Internet of Medical Things).

The terms “IoT in healthcare” and “IoMT” are often used interchangeably. For the purpose of this discussion, “IoT” refers to the internet of non-medical things, such as security systems and asset control that are found in hospitals. “IoMT” refers to connected medical devices, such as heart monitors that track patient status.

Even as healthcare delivery organizations embrace the acquisition of more IoT and IoMT devices, issues such as cost, complexity and security can slow deployment progress. Information captured from active and passive devices raises questions about how and where to manage, process, and store this data. Depending on the data source and type, compliance concerns such as HIPAA, GDPR, and other regulations must be considered. And we can’t forget security. If they’re not sufficiently secured, adding devices to a network also adds more access points for hackers.

Taking a Team Approach to IoT

Healthcare leaders charged with navigating Io(M)T turn to a team approach — from security to workflow, Io(M)T is a journey, not a destination. Involving cross-functional team members early in the decision-making process leads to broader adoption. According to a 2019 survey of IT professionals, Microsoft found that 77% of organizations face unexpected challenges with IoT deployment.[3] Make no mistake, IoT means change, and change management programs demand a team approach.

A project team assembled from key stakeholders — clinical, operational, and even patient advisors — is key to steering an Io(M)T project through successful deployment. This team will frame project goals and outline an evolution of Io(M)T through deployment (and adoption) milestones.

Create a roadmap for intelligently growing an Io(M)T solution. Consider existing "smart" assets already deployed in the hospital and decide strategically what use cases to activate and which devices to add, and where, for the most efficient use of budget and the best outcome. Define Io(M)T solutions that not only fulfill today's needs, but provide the foundation for tomorrow's expansion.

Covered in this e-book:

1 **IoT AND IoMT EXPAND DATA GRAVITY**
The explosion of Io(M)T data requires sophisticated systems to analyze and store it.

2 **DEVELOPING AN INTEGRATED SOLUTION: HOW TO START**
Create a comprehensive Io(M)T solution to take you from now into the future.

3 **SPREAD COSTS BY GROWING THE SOLUTION INTELLIGENTLY**
Where to begin and how to expand an Io(M)T solution over time.

4 **WHAT KINDS OF DATA EXIST NOW, AND WHAT ELSE IS COMING?**
Categories of data (data sets) to consider monitoring.

5 **COMPUTING ALTERNATIVES: AT THE EDGE OR IN THE CENTER?**
Which data should be computed in a data center? Which is needed locally?

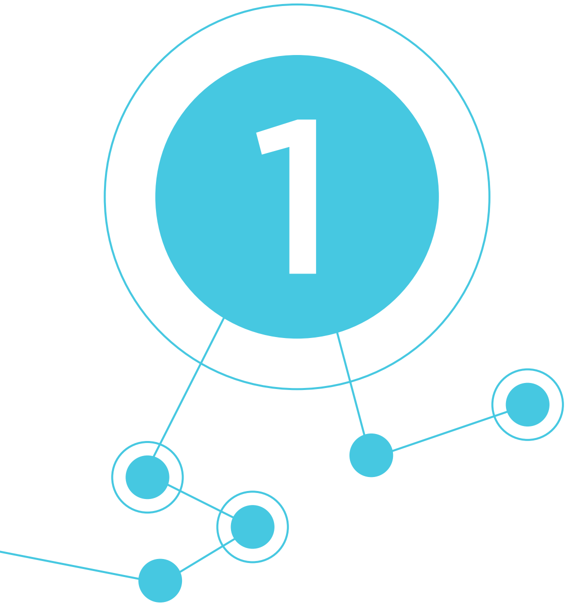
6 **EDGE COMPUTING EASES DATA GRAVITY PROBLEMS**
Moving computing power to the network edge has important benefits for healthcare settings.

7 **DATA SECURITY**
Approach data security in layers, each with a solution that should be built into the device.

8 **WHAT TO LOOK FOR IN AN Io(M)T PARTNER**
In the rapidly evolving Io(M)T market, longevity and experience are important vendor qualities.

9 **KNOWING THE RIGHT QUESTIONS IS AS IMPORTANT AS KNOWING THE ANSWERS**
Key questions to ask the solution development team.

IoT and IoMT Expand Data Gravity



The term “data gravity” was coined to represent the relationship between data and the technology that manages it; more data attracts more technology and software solutions. As data collection increases exponentially, ever-more-sophisticated systems are needed to process, distribute, and store it securely.

An IDC report forecasts that healthcare will grow faster than any other industry in its collection of data, matching the financial services industry by 2025. New data will come from advancements in analytics and imaging technologies and the growing amount of real-time data collected in medical care.[4]

The volume of data collected expands as rapidly as the number of IoT and IoMT endpoint devices and their uses. So do the challenges of managing and securing that data. An integrated Io(M)T solution can provide for current data handling demands while also laying the groundwork for systematic expansion.

Developing an Integrated Solution: How to Start

An integrated Io(M)T solution is one that:

- Integrates IoT and IoMT data collected throughout the hospital or system
- Processes data efficiently
- Provides actionable results where and when they're needed
- Stores data securely
- Does not overwhelm Wi-Fi network capacity or increase latency
- Is expandable in the future
- Includes rules governing all the above processes

What is the best approach to designing, testing, deploying, managing, and growing such a complex solution?

IBM offers this advice:
The integration of connected devices and IT services poses major challenges in networking, communication, data volume, real-time data analysis, and security. IoT solutions involve many different technologies and require complex development cycles, including significant testing and ongoing monitoring.

To overcome these challenges, IT organizations must:

Develop a comprehensive technical strategy to address the complexity

Define a reference architecture for their IoT solution

Develop required skills to design, develop, and deploy the solution

Define their IoT governance processes and policies[5]

In other words, start with the big picture. Assemble a cross-disciplinary team to create institutional policies and structures that will support future expansion of the integrated Io(M)T solution. Designing for the future provides direction for the intelligent growth of an integrated Io(M)T network.

The result is a roadmap for future expansion.

Spread Costs by Growing the Solution Intelligently

Rather than allow the cost of the total solution to slow or prevent its deployment, grow the solution intelligently, using the design roadmap to decide what next steps to take.

A good place to start is by inventorying existing assets to see which could be configured to fit into the overall solution. Hospitals already have many IoT data collection and computing devices throughout their facilities. While they may not currently be connected or configured to work together, a comprehensive Io(M)T solution can be designed to weave legacy equipment into the new network.

Another strategy for gradual growth is investing in new edge computing devices. Intelligent edge devices are cost-effective and can be configured with existing or new data collection endpoints, one area at a time.

ThinkCentre® Nano

What Kinds of Data Exist Now, and What Else is Coming?[6]

Hospital data can be classified into use categories encompassing both IoT and IoMT. Many already are being collected and used, while others may still be on the hospital's wish list. All need to be accounted for in designing an integrated solution.

Here are eight primary data categories and examples of data sets that hospitals may already be capturing.

Administration

- Personnel and patient location services
- RFID technology that enables single sign-on
- Smart meeting room devices that support communication

Asset Management

- Inventory control sensors
- Real-time location of equipment using RFID technology
- Sensors used to allocate operating theaters and patient rooms

Care Delivery

- Bedside equipment monitoring (e.g., ventilators, infusion pumps)
- Next-generation robotics and video equipment that assist doctors in performing surgery
- Telemedicine communications devices that allow remote specialist consultation

Facility Management

- HVAC sensors to control temperature and humidity
- Refrigeration sensors to control temperatures for drugs and tissue samples
- Smart elevators that predict repairs and reduce wait times
- Sensors used to maintain water pressure

Patient Experience

- Check-out instructions and home compliance tracking
- Patient check-in
- Patient orientation and smart floor maps

Patient Monitoring

- Ambulatory EKG monitors and portable EKG machines
- Continuous blood pressure monitoring in critically ill patients
- Oxygen monitors
- Radiation dose monitoring
- Telemetry monitoring
- Wearable devices that track health metrics both in and out of the hospital, aggregating data to give a long-term view of patient health

Safety and Security (Facility)

- Security cameras and systems
- Smoke detectors and fire alarms
- Sensors for measuring levels of oxygen and gases throughout the facility

Safety and Security (Patient)

- Fall risk/detection monitoring
- Telemetry monitoring
- Patient location monitoring (e.g., in-hospital, memory care)
- Radiation dose monitoring

Computing Alternatives: At the Edge or in the Center?

A comprehensive solution must include plans and policies for aggregating, storing, analyzing, securing, and making each class of data actionable.

Which data should be aggregated and computed in a data center? Which is needed locally?

Io(M)T data collected in patient rooms and treatment areas may need to be analyzed and made actionable in real time at the bedside. The data may also need to be anonymized before post-processing, depending on the use case.

For big-picture insights, data can be aggregated in the data center (on-prem or cloud) to analyze with a larger data set collected throughout the building or campus. For example, associating environmental data from HVAC systems (e.g., temperature and humidity levels) with infection rates could reveal underlying causes of outbreaks.

What is Edge Computing?

Edge computing is a solution used to reduce data gravity and make data actionable near the point of collection.

Edge computing distributes computing power throughout the network by replacing passive collection hubs with intelligent edge devices. Rather than passively collecting data and relaying it to servers for processing, intelligent edge devices compute data received from endpoints and indicate needed actions on the spot.

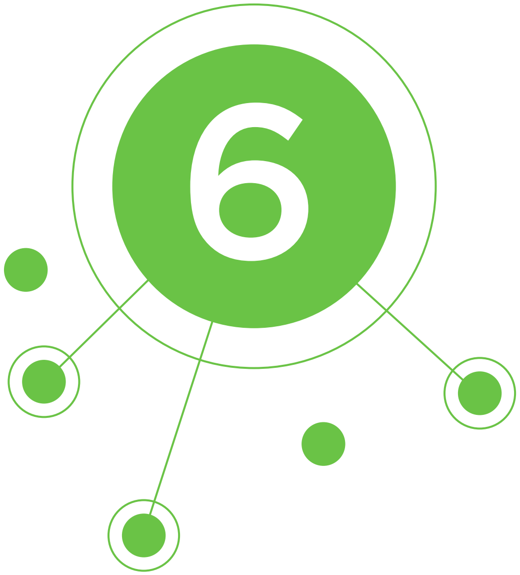
Intelligent edge devices can also distill collected data and send conclusions to the data center for further analysis and storage. Rather than storing all the data from continuous monitoring of a patient's heart rate, for example, the edge device can use that data to report a critical change and alert healthcare providers without storing any data in the data center.

Smart edge devices offload processing and data storage from the data center and bring actionable insights closer to the point of collection.

Data Centers Process and Store Big Data

While edge computing has advantages, it doesn't replace the role of data centers in aggregating data from all points in a hospital or system to provide big-picture insights. System-wide energy use, for example, or the availability of drugs or supplies requires centralized computing. Analyzing hospital-wide trends also helps guide longer-term decisions, such as hiring and purchasing, to assure the health of both the patients and the organization itself.

Edge Computing Eases Data Gravity Problems



Moving computing power to the edge of the network has many benefits that are especially important in hospitals and healthcare settings.

Edge computing allows real-time decision support to be separated from data storage and broader analytics. The result for patient care is reduced latency, faster analytics, and machine learning where and when they are needed.

Navigant Research points out that "...[A] well-designed HVAC system that leverages an edge IoT infrastructure could produce significant savings through its ability to react quickly to subtle changes in air temperature or occupancy levels and intelligently make automated adjustments at the optimal time."[7]

Eliminating the need to upload raw data to a data center for post-processing also saves Wi-Fi bandwidth.

For handling data that is covered by government regulations, intelligent edge computing devices can be individually programmed to comply with regulatory requirements at the point of collection.

Risks of Not Using Smart Edge Computing

In patient care, edge computing keeps the focus on the critical subset of data — that relating to the individual patient — allowing for greater insights and real-time responses.

Analyzing data near the collection point also reduces latency (the time it takes to get actionable information from the computer). The wait for data to be transmitted and analyzed, and results returned, can delay action in critical situations such as surgeries or ICU patient monitoring. It also reduces efficiency in facility IoT system monitoring for use cases including predictive maintenance.

Data Security

Security is one of the top sticking points for healthcare executives in implementing or expanding Io(M)T solutions.

Most healthcare leaders are aware of the benefits in patient outcomes and cost savings that Io(M)T solutions can provide. According to Zion Market Research, the global market for smart medical products will be pushing $67 billion by 2024 as healthcare providers and vendors search for new pathways to improve population health and reduce spending on chronic disease. The report notes that healthcare leaders believe “Smart healthcare products improve outcomes related to diagnostic tools and enhance patient treatment along with improving their quality of life.”[8] But with this tremendous growth comes a greater focus on security.

Healthcare executives know that health systems are prime targets for cyberattacks. In just one month, March 2019, an average of one healthcare data breach per day was reported to the HHS’s Office for Civil Rights. Nearly one million Americans were affected.[9]

Any data point, whether endpoint device or computer, could open the door to a hacker. The more devices added to a wireless network, the more potential access points.

The danger already exists. For years, hospitals have been connecting non-medical IoT devices to hospital wireless networks. Those devices improve security, efficiency, and facility maintenance — but also provide doorways for hackers. HVAC systems, network-connected thermometers in refrigerators used to report temperatures to meet JCAHO (Joint Commission) standards, parking garage cameras, and smart elevators are just a few examples.

How can healthcare organizations both expand Io(M)T solutions and increase the security of existing devices and networks, so a logarithmic growth in devices doesn’t become a logarithmic growth in risk?

7

Approach Device Security in Layers

A useful approach to device security is to think of it in layers. Each layer has its own solution, which should be built into the device.

- Secure the device's firmware and BIOS
- Secure the data on the device
- Control access to the device
- Secure connectivity of the device to the network through network encryption, data pathways, and network security measures

Intelligent edge devices are particularly useful for network security because they form a programmable gateway between endpoint devices and hospital networks.

Each intelligent edge device can be secured to provide a regulated control of endpoints. This control stops any attempted attack at the smart edge device, preventing access to the hospital's wireless network by unauthorized intruders.

Securing devices starts with the vendors who manufacture, sell, update, and maintain them. As with device security on laptops, desktops, and workstations, edge computing devices must also be designed from the ground up for security.

Choose the Right Wireless Connection for the Job

Connecting IoT and IoMT devices doesn't require that every device be connected to the hospital wireless network or ethernet. Other connection technologies can be employed to create more secure, denser IoT environments.

Narrow band IoT (Nb-IoT) applications include facility monitoring, fire and intrusion alarm systems, asset and personnel tracking, and connecting wearable health monitoring devices.[10]

Devices can also be connected to intelligent edge devices or servers using LoRaWAN® technology, which can send data up to nine miles while extending battery life to five to 10 years. The technology is inexpensive and can be secured with end-to-end encryption.[11]

Another alternative is Bluetooth® mesh, a technology designed for creating large networks of devices in which each is connected to all the others. IoT solutions requiring hundreds or even thousands of sensors can be connected using Bluetooth mesh technology without clogging the hospital's Wi-Fi network.

Before Investing in Intelligent Devices, Ask These Questions

Ask vendors how they provide security at every step of the supply chain.

Are suppliers of hardware components qualified?

Are the components controlled and secured?

How secure are the manufacturing facilities and their own computer networks?

Who is programming those devices for delivery? How secure is the process?

Is packaging tamper-proof?

Are shipments tracked?

Are replacement parts secured in the same way?

Updating BIOS and firmware securely is critical to maintaining device security. In hospitals, updates often must be performed while the device is operating. There is no scheduled downtime. So, ask the device vendor: How do you provide secure updates?

What to Look for in an Io(M)T Partner

IoT and IoMT solutions are rapidly evolving, making the future hard to predict and longevity an important criterion in selecting vendors.

Designing, deploying and maintaining an integrated solution involves vendors of endpoint devices, intelligent edge devices, data center computing, wireless networking, and network security. All aspects of the solution must work together seamlessly, reliably, and with minimum latency.

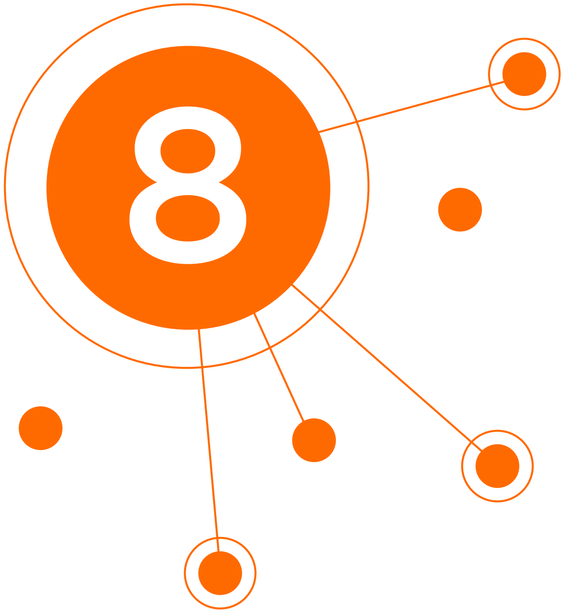
To assure optimal performance, go with experience. Look for vendors who partner with leading brands from across the various industries involved. Ensure a coordinated approach to assessing hospital needs and designing, testing, and deploying solutions.

Longevity comes into play when assessing devices to make the solution work. Hardware investments are expected to last, and be supported, for years. Many vendors in the Io(M)T market are startups — impressive technology, but without the track record to ensure they'll be in business for the long term.

A sound Io(M)T investment strategy focuses on developing a partnership with an established technology market leader. Consider companies known for innovation underpinned by quality and service. Consider each potential partner's financial commitment to Io(M)T solutions and their understanding of IoT's impact on the unique requirements of the healthcare industry, including device and patient safety and security.

According to a KLAS Research report on medical device security:

> "A CISO that recently made a decision told us, 'Ultimately, we chose the vendor we did because we thought they would last in the market. Other than that, the differentiators between any other vendors were negligible.'"[12]



Knowing the Right Questions is as Important as Knowing the Answers

Designing an integrated Io(M)T solution requires input from internal and vendor experts. The following questions offer a starting point for those conversations.

1. What is the best way to handle operational data from IoT devices and medical data from IoMT devices?
   - Should the data be collected, computed, used, stored, and secured on the same network?
   - Do those functions need to be divided, with some placed at the edge and others happening in a central data center?
   - Should data sets from operations IoT devices such as HVAC systems, smart elevators, and asset management be handled differently from data coming from medical devices and wearables used in patient care?
   - What are the data handling parameters for each data set?
2. When do IoT and IoMT solutions need to integrate? For example, if a patient's location sensor detects they've tried to enter a restricted area, should nurses be notified? Do patient room oxygen sensors need to be connected to the HVAC system?
3. If data sets sometimes need to be integrated, are they best stored on the same servers? Processed in the cloud or at the edge? Is there medical data requiring special security or restricted access to comply with federal regulations?
4. What are the primary data sets used in the hospital? The healthcare system? Are they aggregated for system-wide insights? Or do they live in separate data centers?
5. To what extent can legacy devices be used as they are, or retrofitted and connected to smart edge devices or servers?
6. What data is best processed on intelligent edge devices for fast answers and to distill it before transfer to a data center for processing? Where do those intelligent edge devices need to be located? Could some purposes continue to be served by passive edge devices?
7. How can the data be secured, and at what point in the network? What steps can be taken to create a security firewall at the edge, protecting the hospital network from any breach in an endpoint device?
8. What security protocols can be implemented to secure both IoT and IoMT networks throughout the hospital?
9. What criteria are most important to consider in selecting vendors or a vendor group that can support the design, testing, deployment, and ongoing management and expansion of an integrated network solution? What issues might arise down the road that require immediate support during hospital hours — 24/7/365? Which vendor(s) can help ensure that the system's investment in Io(M)T realizes its potential?

An IoMT Solution that Works

Hospital CIOs and IT directors face an enormous job in designing, deploying, and managing integrated Io(M)T solutions. Top concerns include:

- The rapidly growing quantity of data
- The best way to network devices to transmit data
- Which data to process at the network edge and which to process in data centers
- How to provide actionable results with minimum latency
- How to store data securely

This is a team effort requiring input from internal experts and vendors across many areas of expertise and industries.

To assemble that team and steer the project through successful deployment, start by asking the right questions. Use the answers to sketch out the big picture of the desired solution. Then create a roadmap for intelligently growing that solution, starting with assets already in the hospital. Decide strategically what devices to add, and where, for the most efficient use of budget and the best outcome.

Lenovo
Health

Lenovo is a trusted provider of healthcare technology with a 20+ year history of world-class innovation, industry leading partnerships, and more than a decade of proven healthcare experience. Lenovo Health powers tailored care delivery in 160 countries and 1,600 healthcare organizations worldwide.

Lenovo Health's vast computing portfolio supports the administrative, clinical, and remote care needs of healthcare facilities with smart edge, cloud, security, and mobility solutions and accessories that streamline workflow and bring data closer to the patient and clinician.

Learn more about Lenovo Health:
www.Solutions.Lenovo.com/Health

References

1 Bera, Ana. "80 IoT Statistics (Infographic)." Safeatlast.co, February 25, 2019.

2 Bera, Ana. Ibid.

3 IoT Signals Report, MS Azure Survey of 3,233 IT Executives, July 2019.

4 Savvas, Anthony. "Healthcare to create more data than any other industry says IDC." Data Economy, November 29, 2018.

5 Gantait, Amitranjan; Patra, Joy; and Mukherjee, Ayan. Defining Your IoT Governance Practices. January 19, 2018. Updated January 20, 2018.

6 Sharma, Pankaj. How Edge Computing in Healthcare Is Transforming IoT Implementation. Apc.com, December 12, 2017.

7 Edge Computing for IoT in Buildings. Navigant Research, Q4 2018.

8 Global Smart Healthcare Products Market Will Reach USD 66.7 Billion By 2024, Zion Research, January 2019.

9 March 2019 Healthcare Data Breach Report. HIPAA Journal, March 2019.

10 Ray, Brian. What is Narrowband IoT (NB-IoT)? – Explanation and 5 Business Benefits. IoT for All, May 19, 2017.

11 LoRaWAN Technology. St.com. © 2019 STMicroelectronics.

12 Czech, Dan. "Medical Device Security – A Sneak Peek at an Upcoming Report." Klasresearch.com, September 12, 2019.

intel

Lenovo