https://ordr.net/article/iot-healthcare-examples/

10 internet of things (IOT) healthcare examples, and why their security matters

Healthcare devices represent one of the fastest-growing sectors of the IoT market. In fact, the value of this sector—which is sometimes called the Internet of Medical Things (IoMT)—is predicted to reach $176 billion by 2026.

To understand what IoMT means for IoT as a whole, and how healthcare IoT devices need to be monitored and managed, you must understand the multiple ways in which IoT devices can be used for healthcare. While the most popular example of IoT in healthcare is remote patient monitoring—meaning IoT devices that collect patient data such as heart rate and body temperature—there are many other examples of IoT in the healthcare industry.

Here's a look at 10 ways IoT is changing healthcare, as well as how the use of IoT devices for medical purposes impacts IoT security.

Healthcare monitoring devices

IoT devices offer a number of new opportunities for healthcare professionals to monitor patients, as well as for patients to monitor themselves. By extension, the variety of wearable IoT devices provide an array of benefits and challenges, for healthcare providers and their patients alike.

1. Remote patient monitoring

Remote patient monitoring is the most common application of IoT devices for healthcare. IoT devices can automatically collect health metrics like heart rate, blood pressure, temperature, and more from patients who are not physically present in a healthcare facility, eliminating the need for patients to travel to the providers, or for patients to collect it themselves.

When an IoT device collects patient data, it forwards the data to a software application where healthcare professionals and/or patients can view it. Algorithms may be used to analyze the data in order to recommend treatments or generate alerts. For example, an IoT sensor that detects a patient's unusually low heart rate may generate an alert so that healthcare professionals can intervene.

A major challenge with remote patient monitoring devices is ensuring that the highly personal data that these IoT devices collect is secure and private.

2. Glucose monitoring

For the more than 30 million Americans with diabetes, glucose monitoring has traditionally been difficult. Not only is it inconvenient to have to check glucose levels and manually record results, but doing so reports a patient's glucose levels only at the exact time the test is provided. If levels fluctuate widely, periodic testing may not be sufficient to detect a problem.

IoT devices can help address these challenges by providing continuous, automatic monitoring of glucose levels in patients. Glucose monitoring devices eliminate the need to keep records manually, and they can alert patients when glucose levels are problematic.

Challenges include designing an IoT device for glucose monitoring that:
a. Is small enough to monitor continuously without causing a disruption to patients
b. Does not consume so much electricity that it needs to be recharged frequently.

These are not insurmountable challenges, however, and devices that address them promise to revolutionize the way patients handle glucose monitoring.

3. Heart-rate monitoring

Like glucose, monitoring heart rates can be challenging, even for patients who are present in healthcare facilities. Periodic heart rate checks don't guard against rapid fluctuations in heart rates, and conventional devices for continuous cardiac monitoring used in hospitals require patients to be attached to wired machines constantly, impairing their mobility.

Today, a variety of small IoT devices are available for heart rate monitoring, freeing patients to move around as they like while ensuring that their hearts are monitored continuously. Guaranteeing ultra-accurate results remains somewhat of a challenge, but most modern devices can deliver accuracy rates of about 90 percent or better.

4. Hand hygiene monitoring

Traditionally, there hasn't been a good way to ensure that providers and patients inside a healthcare facility washed their hands properly in order to minimize the risk of spreading contagion.

Today, many hospitals and other health care operations use IoT devices to remind people to sanitize their hands when they enter hospital rooms. The devices can even give instructions on how best to sanitize to mitigate a particular risk for a particular patient.

A major shortcoming is that these devices can only *remind* people to clean their hands; they can't do it for them. Still, research suggests that these devices can reduce infection rates by more than 60 percent in hospitals.

5. Depression and mood monitoring

Information about depression symptoms and patients' general mood is another type of data that has traditionally been difficult to collect continuously. Healthcare providers might periodically ask patients how they are feeling, but were unable to anticipate sudden mood swings. And, often, patients don't accurately report their feelings.

"Mood-aware" IoT devices can address these challenges. By collecting and analyzing data such as heart rate and blood pressure, devices can infer information about a patient's mental state. Advanced IoT devices for mood monitoring can even track data such as the movement of a patient's eyes.

The key challenge here is that metrics like these can't predict depression symptoms or other causes for concern with complete accuracy. But neither can a traditional in-person mental assessment.

6. Parkinson's disease monitoring

In order to treat Parkinson's patients most effectively, healthcare providers must be able to assess how the severity of their symptoms fluctuate through the day.

IoT sensors promise to make this task much easier by continuously collecting data about Parkinson's symptoms. At the same time, the devices give patients the freedom to go about their lives in their own homes, instead of having to spend extended periods in a hospital for observation.

Other examples of IoT/IoMT

While wearable devices like those described above remain the most commonly used type of IoT device in healthcare, there are devices that go beyond monitoring to actually providing treatment, or even "living" in or on the patient. Examples include the following.

7. Connected inhalers

Conditions such as asthma or COPD often involve attacks that come on suddenly, with little warning. IoT-connected inhalers can help patients by monitoring the frequency of attacks, as well as collecting data from the environment to help healthcare providers understand what triggered an attack.

In addition, connected inhalers can alert patients when they leave inhalers at home, placing them at risk of suffering an attack without their inhaler present, or when they use the inhaler improperly.

8. Ingestible sensors

Collecting data from inside the human body is typically a messy and highly disruptive affair. No no enjoys having a camera or probe stuck into their digestive tract, for example.

With ingestible sensors, it's possible to collect information from digestive and other systems in a much less invasive way. They provide insights into stomach PH levels, for instance, or help pinpoint the source of internal bleeding.

These devices must be small enough to be swallowed easily. They must also be able to dissolve or pass through the human body cleanly on their own. Several companies are hard at work on ingestible sensors that meet these criteria.

9. Connected contact lenses

Smart contact lenses provide another opportunity for collecting healthcare data in a passive, non-intrusive way. They could also, incidentally, include microcameras that allow wearers effectively to take pictures with their eyes, which is probably why companies like Google have patented connected contact lenses.

Whether they're used to improve health outcomes or for other purposes, smart lenses promise to turn human eyes into a powerful tool for digital interactions.

10. Robotic surgery

By deploying small Internet-connected robots inside the human body, surgeons can perform complex procedures that would be difficult to manage using human hands. At the same time, robotic surgeries performed by small IoT devices can reduce the size of incisions required to perform surgery, leading to a less invasive process, and faster healing for patients.

These devices must be small enough and reliable enough to perform surgeries with minimal disruption. They must also be able to interpret complex conditions inside bodies in order to make the right decisions about how to proceed during a surgery. But IoT robots are already being used for surgery, showing that these challenges can be adequately addressed.

Why security matters for IoT in healthcare

In order to make the most of IoT for healthcare, critical security challenges must be addressed.

Above all, IoT device developers, managers and healthcare providers must ensure that they adequately secure data collected by IoT devices. Much of the data collected by medical devices qualifies as protected health information under HIPAA and similar regulations. As a result, IoT devices could be used as gateways for stealing sensitive data if not properly secured. Indeed, 82 percent of healthcare organizations report having experienced attacks against their IoT devices.

Developing secure IoT hardware and software is one step in addressing this challenge. Equally important, however, is ensuring that IoT devices in healthcare are managed properly in order to protect against data from unmonitored devices falling into the wrong hands. A patient monitoring device that has an older version of software or firmware, or a device that is not properly decommissioned after it is no longer needed, for example, could offer attackers an opportunity to infiltrate a network or steal protected health information.

Proper discovery and classification of all IoT devices on a healthcare provider's network helps guard against this risk. Once IoT device networks are properly identified, classified, regulated, and secured, managers can track device behavior to identify anomalies, perform risk assessments and segment vulnerable from mission-critical devices.

Ordr can help

In a hyper-connected healthcare enterprise, the quantity and heterogeneity of IoT devices creates a complex and increasingly untenable reality for healthcare technology, IT and security organizations. Leaders struggle to understand exactly what's connected to the network, what it's doing, and how to regulate and protect it all.

Ordr Systems Control Engine (SCE) can enable visibility, and security of all of your connected medical devices. It can identify, classify, profile behavior and risk, and secure all medical and IoT assets in your healthcare organization. Once you understand the behavior and communications of every connected device, you can proactively secure them using microsegmentation policies enforced on your existing network and security infrastructure, without touching or modifying the devices. You can even use Ordr to maximize the utilization of all of your connected medical devices.