

Don't let your IoT prescription become a risky affliction

In medicine and healthcare, the Internet of Things (IoT) presents technology companies with both opportunity and risk.



In medicine and healthcare, the Internet of Things (IoT) presents technology companies with both opportunity and risk.



The expanding network of internet-connected objects known as the **Internet of Things (IoT)** is transforming the world, and no industry will be immune. The medical and health sectors, however, may stand to reap the greatest benefits. From wearable devices that tell us how many steps we've taken, to ingestible electronic pills that monitor and transmit vital signs, these products have the potential to help us live healthier, longer lives. The medical sector has even spawned its own acronym for these devices: IoMT, for the Internet of Medical Things. Chronic condition management and remote patient monitoring are currently among the most frequent applications for IoMT.

Payers and providers look to IoT to deliver improvements to the broader healthcare ecosystem. These parties are creating improved patient experiences and enabling operational efficiencies by applying IoT to appointment tracking, patient flow and hospital inventory management. This is just the beginning.

IoT is a component of the emerging field of “digital health,” and also enables it. Increasingly, IoT acts as a backbone for digital health companies focused on clinical support systems, consumer health data analytics, telemedicine and large-scale IT systems designed to manage electronic medical records. Digital health companies are positioned to gain as patients and providers continue to adopt IoT.

Accounting for almost one-fifth of the U.S. economy, healthcare is an attractive target market for IoT applications. However, technology companies commercializing IoT products, component parts or related software should consider the risks related to this emerging technology. As they transmit large amounts of personal health information (PHI), many devices used for medical applications pose unique cybersecurity risks. Additionally, IoT device reliability poses significant risks, as these new technologies may function in ways that challenge existing safety and security standards. Technology executives who closely consider these risks will be **better positioned to protect** their companies and IoT market opportunity.

Mike Thoma

CHIEF UNDERWRITING OFFICER, TRAVELERS GLOBAL TECHNOLOGY

[Introduction](#)

[Why now for IoT in medicine and healthcare?](#)

[Three key categories of IoT devices for medicine and healthcare](#)

[Three risk categories every technology company should understand when developing IoT technology](#)

[Actions to consider for minimizing risk](#)

[Insurance considerations](#)

[How Travelers can help](#)

Important note

The “illustrative risk scenarios” described in this document are intended to facilitate consideration and evaluation of risks, and are not necessarily based on actual events. In addition, these risk scenarios are not a representation that coverage exists or does not exist for any particular claim or loss under any insurance policy or bond sold by Travelers or other carriers. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Some risks may not be insurable. Companies should consult an independent agent or broker to evaluate what coverage is right for them.

The “actions to consider for minimizing risk” described in this document are also intended to facilitate consideration and evaluation of how risks can be mitigated. These are not direct guidance or advice on what actions should be taken. Other actions may be appropriate, depending on the circumstances. Companies should consult an independent agent or broker to evaluate what risk management products or services are right for them.

The reference to any information regarding any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply a Travelers endorsement, recommendation or favoring of such item or organization. Any such reference is for informational purposes only. Any potential user of any product identified is expected to conduct their own due diligence and assessment of the vendor, product or service as appropriate for their needs.

Introduction

The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature internet connectivity. These connected objects range from microscopic devices to large, complex equipment. IoT is now changing the practice of medicine and saving lives. By remotely capturing medical data, facilitating medication delivery and enabling digital health applications, IoT delivers greater convenience and functionality to patients and their physicians. Consider the following examples:

VIRTUAL ORTHOPEDIC REHAB

Breg, a sports medicine manufacturer, has developed the Breg Flex™ sensor device and connected mobile app, which together enable “remote virtual rehabilitation.” Following orthopedic surgery, the technology guides patients through an exercise routine, facilitating a reduction in costs for physical therapy. The activity can be seamlessly recorded in a patient’s electronic medical record.

MAXIMIZING HOSPITAL EQUIPMENT UPTIME

A hardware/software solution from Philips Healthcare, e-Alert, monitors sophisticated Philips hospital equipment to prevent outages. When the system detects something abnormal, a text message is automatically sent to an engineer, who can then act to prevent any serious damage or downtime.

BREATHING EASIER

Asthma and COPD patients may avoid acute attacks by wearing a CoughAware listening device around their neck. When the device detects sounds of an oncoming acute attack, it transmits a text message to a caregiver via CoughAware’s cloud-based software. The device works particularly well for senior and pediatric patients who are not likely to have their own mobile phones.

MONITORING MEDICATION

Vitality GlowCap® is a system that uses drug containers with light and sounds to signal patients to take their medication. A chip monitors when the pill bottle is opened and wirelessly relays alerts to patients, even refilling the prescription with a push button at the base of the lid.

REDUCING EMERGENCY ROOM (ER) WAIT TIMES

Using connected sensors, GE helped a New York hospital track when beds were free, reducing ER wait times by as much as four hours.

SMART WOUND CARE

Researchers have created flexible bioelectronics, or smart bandages, for wounds that require ongoing care, such as burns and bedsores. The bandages will deliver medicine, monitor all the vital signs of the healing process and communicate the information to off-site health professionals.





The possibilities in the IoT market are remarkable, but so are the potential risks to technology companies. Such risks are present for technology companies that produce the IoT products, component parts and related software. However, it's possible to build in safeguards and abate risk while embracing the opportunities created by IoT.

In this issue of the Travelers Global Technology Risk Advisor, we examine the opportunities and risks to companies that are developing IoT technology for the medical and healthcare industries. First, we identify the key factors driving IoT adoption. Then, we discuss three key areas of IoT application within medicine and healthcare. Next, we explore key risk categories for technology companies. We conclude with the actions technology companies should consider to minimize risk exposure, as well as insurance considerations to discuss with an independent agent or broker.

Why now for IoT in medicine and healthcare?

A few key factors are converging to bring IoT to medicine and healthcare. Technology companies that understand these dynamics will be better positioned to capitalize on the market opportunity and protect themselves from related risks.



TECHNOLOGICAL ADVANCEMENTS

Technological advancements enable a wider range of device functionality and facilitate the expanded use of IoT in medicine and healthcare in the following ways:

- **Ubiquitous internet availability:** Improvements in high availability internet mean that more connected products can transmit data in more physical locations. The ubiquity of cellular, satellite and Wi-Fi internet connectivity has given IoT devices exactly what they need: extreme mobility. There are now very few places a device can go where it cannot find an internet connection.
- **Moore's law and the miniaturization of technology:** Gordon Moore, founder of Intel and Fairchild Semiconductor, wrote a paper in 1965 noting a doubling in the number of transistors per integrated circuit approximately every two years. This phenomenon, which came to be known as "Moore's law," has continued on a remarkably consistent path and has had a profound impact on digital electronics, allowing smaller devices to assume greater power.
- **Materials engineering advances:** Progress in developing new advanced materials has facilitated advancements in sensors, actuators, casings and other components used in IoT technology. In many cases, this allows devices to maintain high performance in the wide range of conditions they encounter in medical and healthcare applications.
- **Cloud computing:** The cloud accepts IoT-generated data into vitalized storage, allowing IT teams to efficiently capture terabytes of data for later medical analysis.
- **Big data analytics:** The IoMT produces large amounts of unstructured or semi-structured data on a continual basis. Data scientists and other analytics professionals "mine" the data to extract insights that can improve both healthcare operations and patient outcomes.



CONVENIENCE

IoT enhances healthcare convenience by simplifying tedious, mundane tasks that would otherwise have to be performed manually. Healthcare professionals and administrators essentially "outsource" these tasks to technology, freeing them up to spend their time and intellectual bandwidth on those tasks that can only be done by trained medical personnel. And by making jobs easier, the entire healthcare experience is far more pleasant for patients as well as providers. For example, remote monitoring devices reduce the amount of time patients spend traveling back and forth from their healthcare provider. Also, RFID systems used for hospital equipment and inventory save healthcare workers time locating the tools they need to serve patients.



ECONOMICS

IoT has the potential to significantly impact the economics of healthcare. Research firm MarketsandMarkets™ estimates that IoT applications in human health could have an economic impact of as much as \$158.07 billion by 2020. Politicians, payers and providers have struggled to bring American healthcare costs down to more affordable levels. IoT has the potential to improve healthcare affordability by improving chronic disease management, preventing hospital readmissions, enabling home healthcare, enhancing population health management techniques and improving healthcare operations. (See Exhibit 1 for more information on the potential for IoT to improve healthcare affordability.)



MEDICAL AND HEALTH OUTCOMES

The potential for healthier and longer lives drives much of IoT adoption. For example, IoT promises more comprehensive and systematic monitoring of diabetic patients, opening the door to more effective management of the disease. A personal activity tracker may give a healthy 35-year-old insight on developing a more effective exercise routine, slowing the onset of obesity or other conditions.

How IoT impacts healthcare affordability

IoT represents an opportunity for companies to develop technology that removes or reduces costs from the healthcare system. Consider the following ways in which this is already happening:

CHRONIC DISEASE MANAGEMENT

Chronic conditions like obesity, heart disease, diabetes and asthma drive 86 percent of direct health expenditures. The estimated annual healthcare costs of obesity-related illnesses alone are a staggering \$190.2 billion. New fitness trackers offer style along with health insights to help treat or prevent obesity, including advanced resting heart rate and sleep tracking, along with step counting. Since obesity is often a precursor to diabetes, cloud-based services like Omada Health, which provides enrolled participants with wireless scales, pedometers and exercise bands, help pre-diabetes patients lose weight and reduce the chance of getting diabetes.

PREVENTING HOSPITAL READMISSIONS

Preventable readmissions cost the healthcare system approximately \$17.5 billion annually. According to Hospitals & Health Networks, one study found a 64 percent drop in hospital readmissions for patients whose blood pressure and oxygen saturation levels were monitored remotely with IoT technology.

POPULATION HEALTH MANAGEMENT

Population health analysis efforts are currently limited to health underwriting and risk analysis instead of health management and disease prevention. The IoT can change that. By aggregating and analyzing patient-generated data from large populations, payers and providers can gain insight on cost management strategies related to health management and disease prevention.

EFFICIENT HEALTHCARE OPERATIONS

IoT products and the patient data they provide yield a more efficient patient flow, better management of inventory and the ability to serve more patients who need the facilities and equipment. Developing products that alleviate the costs and overhead in the healthcare ecosystems, while delivering patient comfort and ease of access, holds the most potential for successful adoption.

HEALTHCARE AT HOME

Home healthcare can reduce the length of a hospital stay following a surgery. For example, one day of home healthcare costs about 8 percent of the cost of a hospital visit. Today, connected devices and the data they provide, such as respiration, heart rate and blood pressure, offer a valuable alternative to lengthy hospital stays.

Three key categories of IoT devices for medicine and healthcare

Medicine and healthcare represent a broad and deep opportunity for companies developing IoT technology. Patients, consumers, payers and providers all stand to benefit. The following three categories, each with unique challenges, represent the greatest opportunities for technology companies.

A CONNECTED MEDICAL DEVICES FOR CHRONIC CONDITIONS AND REMOTE CARE

IoT plays an increasingly central role in managing chronic conditions and facilitating remote care. External wearable devices, implanted internal devices and connected stationary medical devices are all being utilized for these purposes. Most in-person doctor visits for chronic conditions are essentially biometric information exchanges between patients and their physicians. They can often be replaced by putting in place the right IoT device.

- Heart monitors detect irregular heartbeats that could signal the onset of a heart attack or stroke. The Medtronic MyCareLink Smart™ patient monitor sends information directly from the embedded monitor to the clinic or the patient's doctor, notifying them of the onset of cardiac arrest. These devices can also be programmed to automatically summon emergency personnel if a patient's cardiac signals fall below critical thresholds.
- For patients over age 65, falls are one of the leading causes of injury and death. Elderly patients with diabetes or early-onset dementia are at greater risk of falling and should consider a fall detection and prevention device. A built-in gyroscope can tell the difference between upright and horizontal body positions, as well as irregular arm movements. If a fall position is detected, the device immediately connects to the internet to send for help, sending GPS location coordinates. Not every senior is suited for an electronic fall detector, but for those whose balance is compromised, this IoT device could be the difference between living independently and an extended stay in a skilled nursing facility.
- Glucose monitors automatically take periodic blood samples and alert diabetes patients when an insulin injection is required. Some even interface with wearable insulin pumps to deliver injections automatically. Even Google has taken up the fight against diabetes by developing a new contact lens that performs double duty as a medical monitor. The lens detects blood glucose levels in a patient's eye fluid, eliminating the need for diabetic patients to finger-prick for blood glucose tests. Readings are sent to online data stores via a micro transmitter embedded into a wireless device thinner than a human hair. The microdevice can also warn the patient and his or her healthcare professionals of a dangerous glucose spike.
- Some smart medical devices work in conjunction with traditionally offline medical equipment. A device called a Propeller (from the company of the same name) attaches directly to a conventional inhaler. When a COPD or asthma patient uses an inhaler, Propeller captures the location and environmental conditions and sends the information to a back-end data store. Through a smartphone interface, the system displays all inhaler uses, giving both patients and care providers a digital snapshot of environmental triggers that caused an episode. With a better understanding of respiratory attack data, patients can better manage their condition and live better quality lives.



B PERSONAL HEALTH AND WELLNESS

Consumers increasingly rely on IoT to take control of their personal health and wellness. These devices don't require a doctor's prescription. In fact, many devices can be purchased in leading consumer electronics stores. Their ubiquity, utility and affordability are enabling physical fitness for consumers around the world.

- Smartphone-connected fitness trackers have become a popular option for facilitating personal wellness. These useful devices have captured the fascination of health-oriented consumers bent on self-improvement. By tracking and reviewing their fitness activities over time, users can make lifestyle changes to improve their overall health and longevity. Wearable fitness trackers like the Fitbit, Nike+ FuelBand and Microsoft Band can detect all user activity throughout the course of a day, not just activity traditionally thought of as exercise.
- Devices are available across the price spectrum. Low-end devices in the \$50 range offer a basic skin sensor, the results of which can only be viewed on a corresponding smartphone app or web report. On the other hand, exercise enthusiasts willing to pay \$300 or more can get a fitness tracker that doubles as a smart watch. With an onboard heart monitor and GPS, the Garmin Forerunner 920 XT can track heart rate, sense foot strikes, tally calories burned while playing multiple sports and send the wearer detailed results via email. It also forwards exercise output readings to a cloud web application, where users can record their activity achievements and even share them with friends via social media.
- Device maker HTC has teamed up with sports apparel giant Under Armour to market the HTC HealthBox. This three-device bundle features the wrist-worn UA Band fitness tracker, the UA Heart Rate chest strap and the UA Scale, a Wi-Fi device that measures not only weight, but also body fat percentage. At a pricey \$400, the trio targets only serious techno-athletes.
- Companies like Juvo are proving that wellness technology doesn't necessarily need to be wearable. Juvo's patented fiber-optic sleep and vitals monitor turns any bed into a smart bed by slipping a flat sensor mat under any mattress, thus removing skin contact and discomfort from the monitoring experience while tracking the user's amount of restorative sleep, breathing, heart rate and movement. It also connects with other smart home components like lights or thermostats to promote healthier sleeping habits.





C IOT TECHNOLOGY FOR THE BROADER HEALTHCARE ECOSYSTEM

Providers and payers are deploying IoT to improve healthcare operations and the patient experience. This trend comes none too soon. As baby boomers continue to reach retirement age, many healthcare facilities will become overrun with patients without a corresponding increase in skilled healthcare workers. Look for IoT devices to handle two important jobs. First, they can increase patient safety and improve experience throughout healthcare buildings. Second, they will handle many repeatable administrative tasks that consume large chunks of time but produce comparatively little direct medical value.

- The BAM Labs Smart Bed Technology® sends hard-to-obtain patient health information to caregivers' computers or mobile devices based on sensors embedded in hospital beds. Monitors can tell whether a patient is up, down, moving or has changed positions. Some of the more advanced models can also record heart rate, respiration, sleep trends and even change pressure points on bed-ridden patients who are unable to move. Data points like these can deliver insights not possible by human observation alone. With access to patient behavior patterns, doctors can detect conditions that could lead to further complications and more surgeries.
- Hospital rooms themselves have become as smart as the beds. The University of Pittsburgh Medical Center features smart room technology by IBM. Connected devices can recognize and greet clinicians as soon as they enter the room. They also offer the following advanced sensory functions:
 - **Patient Screen** manages patient expectations by telling them what events will happen that day and which professionals will be administering to them.
 - **Caregiver Screen** gives doctors and nurses access to pivotal information, including drug allergies and prescriptions. Nurses and aides can easily document patient vital signs on a touch screen, which then updates the electronic medical record.
 - **SmartBoard** replaces standard dry-erase boards commonly found at hospital nurses' stations. It also updates staff on new physician orders or patient care plans.
- Hospital inventory management relies on a delicate supply chain and is often subject to human error. Cardinal Health has developed an RFID smart cabinet that tags model numbers, serial numbers, expiration dates, cost and purchase orders, all of which automatically show up in the hospital's inventory profile. This RFID smart cabinet can perform 20,000 automated inventory counts per year, to near perfect accuracy, without any human involvement. Inventory worries and surprises would be a healthcare concern that remains firmly in the past.
- At Adventist Health System – Florida Division's Orlando-area hospital, real-time location system (RTLS) badges track surgery patients' progress from the pre-op room to the surgical suite to the recovery unit. In the waiting room, family members view real-time process updates on a big-screen TV. The hospital optimizes nurse and doctor staffing levels, based on analysis of surgical patient flow data from the system. The result? Patients and families have embraced the system, as it has improved their experience at the hospital.

3

risk categories every technology company should understand when developing IoT technology

As technology companies pursue the IoT opportunity, they should not forget about the risks. Should IoT software, component parts or finished devices fail to work as intended, a patient can be injured, or sensitive personal health information may be placed at risk. To best manage these exposures, technology companies should carefully consider the following three categories of risk:



Category 1: Bodily injury

Despite the best of intentions to improve medicine and health, IoT technologies can sometimes have the exact opposite effect. These technologies must be used as intended and function properly after public release. Should a device ever fail to operate as planned, technology companies could be liable for resulting injuries or even the death of a user or patient. Those who produce IoT technology should understand their exposure to bodily injury risk due to defective design, a manufacturing defect, product misuse or a failure to warn consumers about a potential danger related to using the product.

ILLUSTRATIVE RISK SCENARIOS

INACCURATE HEALTH RECORDS

A hospital implements a new system of devices for remotely monitoring the status of patients during their first week home after certain invasive medical procedures. During the course of entering data for one patient following major surgery, a software glitch in the new system causes the deletion of another patient's allergy records. Doctors view the altered records and give the affected patient medication that leads to an allergic reaction. The software company is sued for the bodily injury caused by failing to maintain accurate records.

CIRCULATORY SUFFERING

A hospital equips its patient rooms with connected smart beds for patients who cannot move on their own. The beds provide data on sleep duration, quality and other metrics to a patient's electronic medical record. The beds are programmed to measure how long a patient has been lying in one position and to adjust the pressure on the body accordingly. However, a sensor on the bed malfunctions, causing the bed to apply more pressure (instead of less) to an immobile patient, resulting in painful bedsores and exacerbating circulatory problems. As a result, the patient requires an additional surgery to relieve pain and circulation problems. The bed manufacturer is held liable for the cost of the additional surgery.

SWALLOWABLE MISINFORMATION

A doctor prescribes pills with a swallowable chip to verify compliance of a patient with a memory impairment. But a flaw in the device design prevents the transmitter from sending compliance data to the physician. Unaware that the patient is not taking his medication, the doctor does not get the opportunity to intervene, causing the condition to worsen. The patient's condition deteriorates to the point where he needs expensive surgery. The patient sues the company that made the connected pill for failure to transmit his compliance data in a timely fashion.



Category 2: Technology errors and omissions

A purchaser of IoT technology may sustain economic losses from the failure of the technology to work as intended, due to an error, omission or negligent act in the design of that technology. In such cases, the purchaser may claim lost profits or business disruption. Defense expenses alone in these cases can be catastrophic to a technology business. With each new IoT application, the potential for economic losses increases. Companies who understand the unique nature of this risk category can better protect themselves from liability claims.

ILLUSTRATIVE RISK SCENARIOS

MISSED MEDICAID DEADLINE

A cyber thief is able to exploit a security weakness in a connected heart monitor to gain access to the practice's automated accounting and billing system. The intruder deletes large quantities of electronic health records. Because the physician's office doesn't maintain daily backups, they must manually re-enter data from procedures they have already performed. The process takes so long that the time limit for Medicaid reimbursement expires, causing them to lose payments from government agencies. The failure is traced back to the security vulnerability in the connected heart monitor.

OVERSTATED FITNESS TRACKER

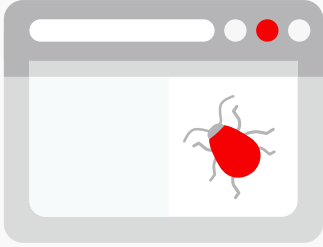
A health insurer offers an incentive to its customers to become more active by using a fitness tracker. Any customer who walks 8,000 steps per day and allows the insurance company to electronically verify his or her activity qualifies for the discount. A glitch in the fitness tracker software causes the program to overstate steps, causing the company to give more discounts than they should. The insurance company discovers the anomaly, investigates and attributes the financial loss to incorrect step counts as a result of external fitness tracker manipulation.

COMPLICATION DETECTION FAILURE

After a heart bypass operation, a patient is sent home with a wearable heart monitor that communicates cardiac data to medical staff over the internet. However, the monitor fails to communicate important heart readings which would alert physicians that the patient is experiencing a minor complication. Because the problem goes undetected, the patient doesn't get the proper treatment in a timely manner. Her condition worsens to the point where she must be readmitted to the hospital for an emergency procedure. Because the readmission occurs within a brief period after initially being sent home, the hospital must absorb a portion of the cost of the second admission. The hospital sues the device manufacturer for its financial loss caused by the device's failure to detect the complication.



Category 3: Cyber risk



Cyber risk is often defined as the risk of financial loss, business interruption or reputational damage due to an organization's failure to properly secure the data held within its information systems. While IT is often the focus of cyber risk, and top management is ultimately held responsible, everyone in the entire company plays a vital role in securing client data and protecting intellectual property.

As profit potential for medical device makers is on the rise, so is the risk of cyber attack. Thieves find protected medical information a particularly attractive target and have come up with more elaborate schemes to break into IoT-based information systems. A recent PricewaterhouseCoopers survey shows a 192 percent increase in cyber attacks on embedded devices and a 241 percent increase in operational system attacks in the healthcare sector. And while businesses are investing in greater safeguards to defend their electronic perimeters, companies increased their spending on cybersecurity by only 8 percent over the previous year.

ILLUSTRATIVE RISK SCENARIOS

THEFT OF PERSONAL HEALTH INFORMATION (PHI)

A heart patient's wearable cardiac monitor is programmed to upload batches of medical readings to a cloud data store at periodic intervals. Engineers in charge of cloud security become overwhelmed with concurrent deadlines and fail to properly configure a security patch, creating a vulnerability. A hacker gains entry, then steals and sells the patient's sensitive health data.

POLITICAL PILL PUBLICATION

A high-profile politician with a sensitive mental health prescription history takes edible "smart" pills to monitor both medication regimens and health issues. A hacker gains access to the politician's pill data in the middle of an election season and sells it to a tabloid. The politician sues the device maker for failure to protect PHI.

THUMB DRIVE THEFT

A major pharmacy chain tracks drug inventory using IoT devices. A rogue employee assigned to the inventory control function becomes familiar with the inventory control sensors and discovers a way to access customers' PHI using the database credentials assigned to the sensor software. The employee downloads sensitive information to a thumb drive, takes it home and sells it to interested parties. A customer discovers his or her information on a third-party website and sues the pharmacy for failure to secure sensitive information.



Actions to consider for minimizing risk

IoT offers patients and the broader healthcare ecosystem exciting new possibilities for improving healthcare delivery and outcomes. However, as technology companies develop, manufacture and commercialize IoT, they expose themselves to significant risks. Companies can be held liable for bodily injury, economic losses to third parties and the failure to properly secure data. Fortunately, there are several actions that companies can consider to minimize their exposure to these risks.

CONSIDER APPROPRIATE QUALITY AND RISK MANAGEMENT SYSTEMS

Companies manufacturing IoT devices for medical and healthcare uses should be aware of and adhere to appropriate quality and risk management systems. This will help to ensure that their products consistently meet requirements and specifications. Manufacturers should develop product requirements to achieve product safety and efficacy, and they should develop procedures and methods to design, manufacture and distribute their products.

- For IoT products **classified as medical devices** by the FDA, **21 CFR 820** outlines Quality System Regulation (QSR) requirements for medical device manufacturers. In addition, **ISO 13485**, which is published by the International Organization for Standardization, also applies to medical device quality systems.
- For IoT products **not classified as medical devices** (including many health and wellness devices and devices within the broader healthcare ecosystem), manufacturers should consider **ISO 9001:2015**, a widely used quality management system. Also, **ANSI Z535** outlines a system for alerting users to possible harm via product labels and instructions.

Direct and reputational costs from product losses can cripple companies, sometimes endangering their very existence. Regardless of the quality system adopted, device manufacturers should consider the following steps to ensure device safety and security:

Conduct robust hazard analyses

Methods such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), and hazard and operability study analysis (HAZOP) can be used by device makers to assess potential hazards at different points in device development and commercialization. Companies should not ignore issues that can be introduced during processes such as manufacturing, packaging, labeling, storage or transport.

Conduct design reviews

Firms involved in IoT device development should assess the likely frequency and severity of all identified potential hazards their devices could cause. All firms in the development and production chain should seek to eliminate high-severity hazards and reduce the potential for medium- and low-severity hazards. Companies should assemble a diverse team that includes personnel outside of the design process to generate potential mitigation solutions.

Conduct extensive testing

Product manufacturers should not only test their own devices, but also any related software or peripheral hardware they may be using. Software and firmware developers should implement a system of continuous integration to detect bugs as early as possible in the build phase where they are easiest and least costly to fix.

Develop clear safety and use instructions with conspicuous warning labels

Companies should provide users with clear, unambiguous written instructions on the full range of device usage. This includes providing visual depictions of proper device use, as well as instructions on what to do if a device malfunctions.

BUILD IN CYBERSECURITY

A lack of cybersecurity in devices creates the potential for unplanned and costly events. A device designed to deliver medication or monitor a facility's conditions could be breached, resulting in serious consequences to patients or property. With the right efforts, companies can protect themselves by incorporating simple, yet effective security features into IoT technology. Consider the following steps to minimize exposure to cyber risk:

Encourage input from IT security professionals

Cybersecurity professionals should communicate with all business functions responsible for the development and commercialization of IoT technology. To build in security from the start, security engineers should reach across organizational reporting relationships. Every phase of IoT device development should interface with security engineers, including product design, development, testing and customer service. Organizational silos should not prevent security professionals from providing critical input for the finished product.

Application security patches

A major part of the software application development lifecycle (SDLC) is maintenance. The “always-on” nature of the IoT makes patches and service releases particularly challenging because there is no concept of scheduled downtime; updates need to be applied when all devices are in use. Because security threats evolve over time, application developers must design their apps in ways that can accommodate a real-time “push” service pack installation without compromising performance levels during the installation.

Physical security

Some IoT devices are very small, making it easier for thieves to steal them unless they are physically secured or otherwise out of a potential thief's reach. If the device has any sort of internal storage mechanism, the data on the device at the time it is stolen will also be at risk. Device makers should anticipate the possibility of a device being stolen and implement warning mechanisms to notify the owners and wipe the local data cache in the event of a device theft.

Bluetooth encryption

Bluetooth offers an encryption API when exchanging data between a device and its target data store, but few companies take advantage of it because it decreases battery life. Consider enabling it for more effective security.

Ensure backward compatibility

Sensor hardware is only half of what is necessary to make the IoMT work properly. The other half is the software that receives data from sensors in the field. Embedded devices are very durable, and may outlive the algorithms that power them. IT leaders should take steps to ensure that this does not happen. Make sure that any new algorithms or program changes are backward compatible to the sensors they are designed to accept data from.

Custom security level

Encourage physicians and nursing staff to choose higher levels of security when they install their device or pair it with their smartphone. Users seldom consider security when wearing their devices, so defaulting to the least secure settings opens them up to hackers.

Identity management

In the typical corporate local area network (LAN), two basic building blocks of security are authentication and authorization. Security algorithms allow work to be done by personnel who have input their network passwords by hand. This is not possible with IoT nodes, so input validation must be performed some other way. The National Institute of Standards and Technology (NIST) has recently chosen the compact SHA-3 as the new algorithm for the so-called “embedded” or smart devices that connect to electronic networks but are not full-fledged computers. Other authentication methods to consider include geographic IP filters, strong identities and delay-tolerant networks.

Secure the cloud

Data is often transmitted from a sensory device to a smartphone and then to a cloud data store. Virtualized clouds can secure data with multiple diverse operating systems, each operating within a different security context. Banks often secure depositor payment details this way; companies producing IoT technology should consider similar functionality.

Require strong passwords

Devices should be designed to disallow default passwords and should instead require strong passwords before the device can be deployed.

Encrypt critical data elements

The most critical pieces of data transferred between IoT devices and data stores are often user IDs, passwords and PIN numbers. Astoundingly, most devices transmit these data elements in plain text with no encryption at all.

Remote erase feature

Consider building in the option to remotely erase and/or disable a device if it is ever lost or stolen. This feature comes standard on many late-model smartphones.

For additional insights on ensuring cybersecurity for IoT, technology companies should consult the following resources:

- **Strategic Principles for Securing the Internet of Things (IoT)**, published by the U.S. Department of Homeland Security
- **Postmarket Management of Cybersecurity in Medical Devices**, published by the U.S. Food and Drug Administration

EVALUATE COMPANY CONTRACT PRACTICES

From time to time, even well-designed products fail to perform as expected. In those rare cases, a deficiency could have unfortunate side effects that manifest themselves in high-dollar liability claims. Companies can manage their exposure to technology errors and omissions risk by ensuring that they contractually transfer risk where possible. To do this, technology companies should consider the following specific contract provisions:

Limitation of liability

This provision disclaims liability for certain types of damages – usually incidental, indirect consequential and special damages. In the event of actual or threatened litigation, these provisions can become very useful in minimizing ultimate exposures.

Damage caps

These provisions limit the amount of otherwise recoverable damages. The limitations can be defined in terms of a specific dollar amount or an amount to be determined, depending on specific factors set forth in the contract.

Disclaimer/limitation of warranties

This provision identifies the warranties provided, disclaims or limits those warranties not provided, and identifies the remedies available in the event the product or work does not comply with the warranties provided.

Integration

This provision identifies the documents that comprise the parties' contract and will also limit the parties' reliance on documents and information outside of the contract.

Contractual risk transfer and defense/indemnity provisions




Provisions like these can shift risk to other parties.



Insurance considerations

It is impossible to predict the many ways in which technology companies could find themselves liable should IoT technology fail to operate as expected. While these risks cannot be eliminated, they can and must be managed. To help decrease exposure, technology companies should investigate insurance options for the categories of risk described in this issue of the Travelers Global Technology Risk Advisor.

The following table recounts the key risk categories and illustrative risk scenarios noted earlier, along with information on relevant insurance coverage to protect against potential liability.

		
Risk category	Illustrative risk scenario	Relevant insurance coverage to evaluate with an agent or broker
Bodily injury	<ul style="list-style-type: none"> • Inaccurate health records • Circulatory suffering • Swallowable misinformation 	Product liability coverage provides coverage for physical harm to a person arising out of a product manufactured, sold, handled, distributed or disposed of by you.
Technology errors and omissions	<ul style="list-style-type: none"> • Missed Medicaid deadline • Overstated fitness tracker • Complication detection failure 	Errors and omissions (E&O) liability coverage protects against damages that you must pay because of economic loss resulting from your products or your work, and caused by an error, omission or negligent act.
Cyber risk	<ul style="list-style-type: none"> • Theft of personal health information (PHI) • Political pill publication • Thumb drive theft 	Cyber liability and cyber-related first-party coverages provide protection for critical cyber risks. Liability coverage options vary, but most include coverage for loss caused by the failure to prevent a security breach. First-party expense coverages can include forensics, data restoration, business interruption, extortion, computer and funds transfer fraud, and public relations and breach notification expenses.

Each company's security requirements are unique, so few insurance policies come standard. Likewise, not all risks may be insurable. It is important to contact your independent insurance agent or broker to discuss your company's unique insurance requirements.

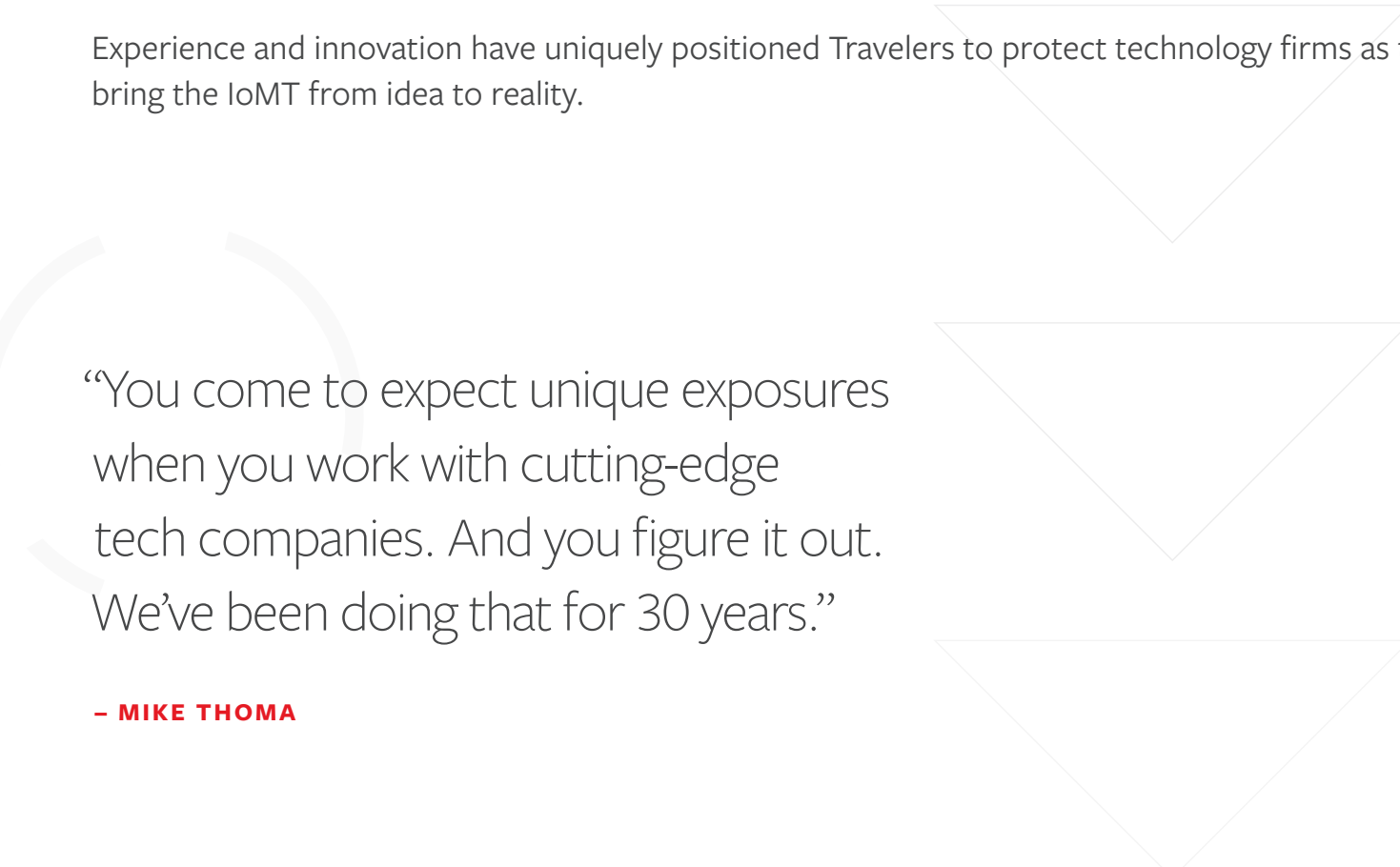


How Travelers can help

Travelers understands the unique needs of technology firms. We often insure what other carriers will not, because we've been protecting tech companies longer than most. So, as you work on the next groundbreaking IoT technology, Travelers will be there to help manage the risks with the right insurance products.

Travelers stays ahead of technology industry risk. From the rise of PCs to the Y2K scare to the internet economy, Travelers continues to evolve with effective options to provide technology companies with important insurance coverage for exposures as they continue to innovate. Mike Thoma, Chief Underwriting Officer for Travelers Global Technology, says, "You come to expect unique exposures when you work with cutting-edge tech companies. And you figure it out. We've been doing that for 30 years."

Experience and innovation have uniquely positioned Travelers to protect technology firms as they bring the IoT from idea to reality.



"You come to expect unique exposures when you work with cutting-edge tech companies. And you figure it out. We've been doing that for 30 years."

– MIKE THOMA

For more information, contact your independent insurance agent or broker, or visit us on the web at travelers.com/technology.

References

Parmar, Arundhati, “Here’s the latest entrant in the Internet of Things healthcare market,” MedCityNews, Mar 22, 2017, accessed Apr 2017, <http://medcitynews.com/2017/03/heres-latest-entrant-inter-net-things-healthcare-market>

Thompson, Cadie, “As healthcare costs rise and patients demand better care, hospitals turn to new technologies,” Oct. 26, 2016, <http://www.businessinsider.com/how-hospitals-are-using-iot-2016-10>

O’Connor, Mary Catherine, “A Wearable That Listens for Troubling Coughs,” July 1, 2016, accessed Nov 2016, <http://www.iotjournal.com/articles/view?14687>

“Vitality GlowCap®,” Vitality Company, 2016, accessed Dec 2016, <https://nanthealth.com/vitality/>

Heck, Charlie, “Not Just a Band-Aid: How ‘Smart Bandages’ Will Change Medicine,” Live Science, April 21, 2015, accessed Nov 2015, <http://www.livescience.com/50559-smart-bandages-use-artificial-intelligence.html>

“IoT Healthcare Market worth 158.07 Billion USD by 2020,” MarketsandMarkets, 2016, accessed Dec 2016, <http://www.marketsand-markets.com/PressReleases/iot-healthcare>

“Chronic Disease Prevention and Health Promotion,” CDC, 2016, accessed Dec 2016, <http://www.cdc.gov/chronicdisease>

“Economic Costs of Obesity,” National League of Cities, 2016, accessed Dec 2016, <http://www.healthycommunitieshealthyfuture.org/learn-the-facts/economic-costs-of-obesity/>

“Omada Health and Humana Partner to Reduce Diabetes Risk in People with Medicare,” Omada Health, Nov 2015, accessed Dec 2016, <https://www.omadahealth.com/news/omada-health-and-humana-partner-to-reduce-diabetes-risk-in-people-with-medicare>

Krawiec, R., Nadler, J., Tye, E., Jarboe, J., “No appointment necessary: How the IoT and patient-generated data can unlock health care value,” Deloitte University Press, Aug 2015, accessed Dec 2016, <https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-health-care-industry.html>

Glaser, John, “How The Internet of Things Will Affect Health Care,” June 4, 2015, accessed Nov 2015, <https://www.hhnmag.com/articles/3438-%20how-the-internet-of-things-will-affect-health-care>

“Peace of Mind is Close at Hand,” Medtronic, 2016, accessed Dec 2016, http://www.medtronic.com/content/dam/medtronic-com/01_crhf/cc/pdfs/RevisedFlyer.pdf

“Digital Contact Lenses Can Transform Diabetes Care,” The Medical Futurist, Apr 2016, accessed Dec 2016, <http://medicalfuturist.com/goggles-amazing-digital-contact-lens-can-transform-diabetes-care/>

“What is Propeller?,” Propeller Health, Sep 2013, accessed Nov 2016, <https://www.youtube.com/watch?v=6CH1lxmwUJs>

“Garmin Forerunner 920XT Heart Rate Monitor Bundle,” REI Co-op, 2016, accessed Oct 2016, <https://www.rei.com/product/881936/garmin-forerunner-920xt-heart-rate-monitor-bundle>

Comstock, Jonah, “CES 2016: Running list of health and wellness devices,” Mobile Health News, Jan 2016, accessed Nov 2016, <http://www.mobilehealthnews.com/content/ces-2016-running-list-health-and-wellness-devices>

“Medical Smart Bed Applications,” BAM Labs, 2016, accessed Aug 2016, <http://bamlabs.com/applications/>

Cerrato, Paul, “Hospital Rooms Get Smart,” Information Week, Oct 2011, accessed Aug 2016, <https://www.informationweek.com/healthcare/%20clinical-information-systems/hospital-rooms-get-smart/d/d-id/1100822>

Saghbini, Jean-Claude, “The Internet of (Very Valuable) Things,” April 5, 2016, accessed Nov 2016, <http://www.cardinalhealth.com/en/essential-insights/the-internet-of-things.html>

Sutner, Shaun, “Internet of Medical Things improves patient experience,” Nov. 9, 2016, accessed Nov 2016, <http://internetofthingsagenda.techtarget.com/feature/Internet-of-Medical-Things-improves-patient-experience>

“Transformation and turnaround in cybersecurity: Healthcare Payers and Providers, Key findings from The Global state of Information Security® Survey 2016, PWC, Oct 2015, accessed Aug 2016, <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-healthcare-providers.pdf>

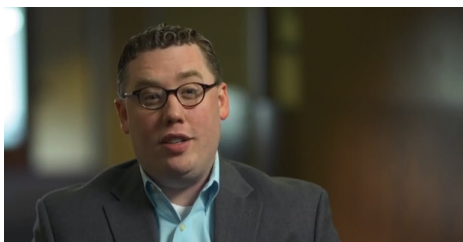
U.S. Department of Homeland Security, “Strategic Principles for Securing the Internet of Things (IoT),” Nov. 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

U.S. FDA, “Postmarket Management of Cybersecurity in Medical Devices,” Jan. 22, 2016, <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>

Risk expertise for the technology industry



Travelers has been insuring technology companies for more than 30 years. Hear directly from Travelers technology industry experts, using the links below.



MITCH FOSTER II
ON TELECOM:
travl.rs/1cgWzik



KIRSTIN SIMONSON
ON INFORMATION TECHNOLOGY:
travl.rs/1PL9YBL



PATTY NICHOLS
ON MEDICAL TECHNOLOGY:
travl.rs/1FVhMwf



JILL DUFFY
ON GLOBAL RISKS:
travl.rs/1FVhhIL



MIKE THOMA AND RONDA WESCOTT
ON INSURING TECHNOLOGY COMPANIES:
travl.rs/1F8WjZR



RYAN STROUTH AND MIKE DEHETRE
ON EMERGING TECHNOLOGY:
travl.rs/1BnJyKw



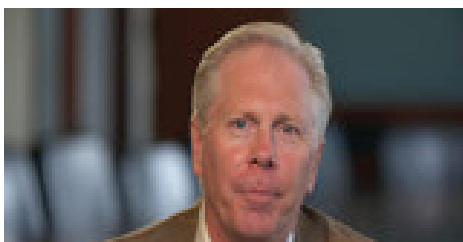
KIRSTIN SIMONSON AND CLAIRE KORNEGAY
ON CYBER RISKS:
travl.rs/1J3jASH



MITCH FOSTER II
ON ELECTRONICS MANUFACTURING:
travl.rs/1Fep5cv



EILEEN KAUFFMAN
ON CLEAN TECHNOLOGY:
travl.rs/1LGy5f8



MIKE THOMA
ON LARGE TECHNOLOGY COMPANIES:
travl.rs/224uxN5



LINSEY MCDONALD
ON TECHNOLOGY RISK CONTROL:
travl.rs/1RmABNd



JERRY GALLIVAN
ON TECHNOLOGY CLAIM:
travl.rs/1OtUUCI



Travelers understands the unique needs of technology firms. We often insure what other carriers won't, because we've been protecting tech companies longer than most. So as technology companies expand globally, Travelers will be there to help manage their risks with the right insurance products.



travelers.com

The Travelers Indemnity Company and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© 2017 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. BTCWH.0005-D New 11-17