WWW.SPKAA.COM

Navigating Compliance and Cyber Security Concerns in Smart Medical Devices

SPK and Associates

A COMPLETE OVERVIEW OF SMART MEDICAL DEVICES, THEIR DEVELOPMENT AND THEIR COMPLIANCE CONSIDERATIONS.

While the Internet of Things offers great opportunities both for businesses and consumers, compliance and security must be thought through carefully from the very beginning. Otherwise, potentially expensive and organizationally painful changes will have to be made after a large investment of time and money. This is an introduction into the challenges presented by the Internet of Things for the medical device industry.

The Internet of Things is changing the nature of medical devices and medical device innovation. However, the changes to the industry are only beginning as Internet of Things technologies are still in their infancy. What's more, the nature of FDA regulations complicates matters greatly. While "dumb" medical devices have fairly straightforward, cut-and-dry process, intelligent, Internet-connected medical devices have a much more complicated path toward FDA approval. Put simply, the typical path toward FDA approval is one that can discourage innovation. This can make your business unsure of how to -- or even if to -- include new innovations in your medical devices despite the positive applications for end users.

The main difficulty from everyone's perspective is the new abilities of smart medical devices. This might sound counterintuitive, but consider what intelligent medical devices do. Intelligent medical devices can collect, store and transmit data. "Dumb" medical devices can collect data and, to some extent store it, but it's probably more accurate most of the time to say that they merely display data. These new capabilities provide legitimate problems of security and privacy for end users, as well as safety. They also create potential compliance headaches as the FDA approval process is much less cut and-dry for smart devices than it is for "dumb" ones.

Related to the easier approval and compliance paths, "dumb" medical devices possess one simple edge over intelligent medical devices: They can't be hacked, because there's nothing really there to hack. There's some firmware and maybe a rudimentary operating system. On the other hand, connected medical devices have varying degrees of insecurity at each connection, from firmware, to operating system, to applications, to various communications protocols. Once the device's security is breached at one of these connections, patient information can be stolen and the device itself can be made to malfunction.

Such risks are the obvious cause of the recent attention and updated premarket guidance from the FDA (October, 2018). These are helpful steps towards mitigating some of the security risks inherent in connected products. Indeed, almost immediately prior to the updated standards in October 2018, a study released in August 2018 slammed the fast track approvals process as ineffective at protecting consumers.

The specter of a large-scale medical hack is no longer in the realm of science fiction. There was a large-scale and long term attack against medical records in Singapore. Fully 1.5 million (25 percent of the country's population) were impacted by the attack. Theoretically, the attack, which lasted from May 1 2015 to July 4 2018 could have been a lot worse. There is no evidence that any of the information was tampered with, which, in the case of data used by connected medical devices, could have deadly consequences for patients.

Navigating Updated Guidelines

The updated guidelines explicitly mention shortcomings in previous guidelines due to rapidly evolving technology. To that end, the guidelines are updated to employ a more holistic, risk-based approach to securing medical devices. The FDA now recommends the following for all medical device manufacturers developing new treatments:

- Identifying assets, vulnerabilities and threats
- Assessing the impact of identified vulnerabilities and threats on both device and patient
- Likelihood assessments of all threats
- Risk mitigation strategies
- Residual risk and risk acceptance criteria

The guidelines go further, including specifications on preventing unauthorized access, the ultimate security flaw. Authentication rules and encryption are just two of the guidelines for connected medical devices. The guidelines further recommend limited access for trusted and authorized users only. Where security flaws exist or compromises occur, there must be a plan in place to rapidly respond to any problems.

Worse even than this is the specter of more personal attacks against individual users. Dick Cheney reportedly had the security on his connected pacemaker beefed up for extra security, but this was merely a precaution. Johnson & Johnson insulin pumps had a security flaw so dangerous customers had to be warned. Not only can the information be stolen, thus breaching privacy, we now live in a world where hackers could potentially commit murder by accessing a patient's medical device, or extort them. Ransomware attacks should illustrate quite plainly that there is little hackers will not do.

So with all of this downside, why would anyone want to make a smart, connected medical device? The big appeal is real-time monitoring of patient conditions. Connected medical devices can spot potentially fatal medical problems before even trained physicians can. Oftentimes these devices connect wirelessly, making them even more convenient than their "dumb" counterparts. Doctors can make adjustments to equipment such as pacemakers without invasive procedures, reducing medical costs and patient hassle.

Indeed, the tech has moved very quickly. Apple includes an electrocardiogram (ECG) app with their most recent Apple Watches. This would have been science fiction even a year ago.

More mundane household applications, such as pill bottles that email and remind patients to take their daily dose, have already been rolled out. In fact, connected devices are probably far more common than you might realize. A recent study showed that there are between 10 and 15 smart medical devices for every hospital bed in the United States. That's a revolution in healthcare, but it's also a ripe field of attack for potential hackers and other cybercriminals.

At the macro level, connected medical devices can collect data on a massive scale. This new data will revolutionize the field by providing insights that were hitherto impossible. Smart medical devices connected to the Internet of Things will revolutionize training in the medical field. It also provides a ready-made target for hackers looking to exploit all of that valuable medical information for nefarious purposes.

Closer to your end of the supply chain, failure to obtain proper FDA clearance can be, to put it mildly, a big headache. Rolling out a new device without proper FDA clearance could mean a total halt to all production while you backtrack, trying to fix compliance issues you should have worked out before production even started. Even without a hack, adding simple new features to medical devices can result in potentially fatal consequences without rigorous testing.

New features must be thought about from the following perspectives:

1. **Goals and Aims:** This is an area which is so easy to skip over, but absolutely essential. Why are you adding this new feature? What do you hope to obtain from it? What advantages does it offer to the end user?
2. **Technology and Talent:** What new technology must you deploy to meet your goals and aims? What talent must be employed to do so? Do you already have all of that talent in house? Does it make sense to hire new talent or simply to contract outsiders?
3. **Vulnerabilities and Exploits:** You must consider every potential vulnerability and exploit the new feature will introduce into your device. Then you must consider how to best protect those vulnerabilities. This might require hiring outside talent to have a fresh set of eyes on the product.

When these bases are covered, only then can you start working on the development of your devices. The problem many organizations encounter is tight deadlines and the rapidly increasing time-to-market schedule. For smart medical devices, it might not be possible to meet the strict development schedules that you're used to. Intelligent features might have to be added after the current cycle if you are trying to meet a tight deadline.

Smart medical devices generally contain the following changes:

- **Robust Operating System:** Operating systems on smart medical devices must have operating systems far more robust than those in "dumb" medical devices. This is necessary to accommodate the rest of the "smart" aspects of the device.
- **Applications and Tools:** Applications and tools will allow you to tailor services to the end user with greater precision and accuracy. You will be able to provide a wider array of services than your current devices are able to provide.
- **Storage:** Information can be stored on medical devices for as long as you need. This requires both hardware for storage and software to manage the storage.
- **Transmission:** One of the most promising features of smart medical devices is Internet connectivity. Smart medical devices can transmit the information stored to the cloud, allowing for more secure storage as well as tracking through big data analytics.

To handle each of these individually, as well as make them cooperate, additional computing power is needed. Each also requires additional FDA oversight to ensure compliance.

There are five tiers to FDA compliance as a whole:

- **Applications:** Applications include visualization, business system integration and the development environment. These must be secured with application identity and access management.
- **Cloud Services:** Your cloud services require databases, storage, device management and monitoring, event processing and tactical analytics for these events, as well as more advanced forms of analytics for data coming in and out of the cloud. Cloud services further require encryption and privacy management.
- **Communication:** Data stored on the device must be transmitted to the cloud. This can happen over one or more protocols, each of which needs its own privacy and encryption features.
- **Devices:** Intelligent medical devices frequently come enabled to connect with other devices. This requires additional features, including protection for each additional physical device connected**.**
- **Security:** Each point of contact is a potential security vulnerability. Your engineers or contracted talent must be able to secure the entire chain of transmission at each point of contact.

Development of smart medical devices connected to the Internet of Things occurs in five main stages:

- **Business Case and Justification:** As stated above, there can often be delays when adding new features to medical devices, so it's important to create a strong business case from the beginning. Because seemingly simple features can complicate development enormously, it's important to evaluate precisely why you are adding the features you are adding.
- **Vendor Evaluations:** There are over 600 IoT platforms available on the market today, some of which will be useful, others of which will not be. You need to address what you can build in house and what has to be outsourced. You also need to evaluate what you can just buy versus what needs to be built. Once there is agreement among developers to buy, you then need to evaluate which vendor provides the best return on investment.
- **Proof of Concept:** Your proof of concept includes detailed security analysis using the STRIDE Model.
- **Pilot:** During pilot, you will use device simulators, which allow you to check integration and skills testing before going to market. You can run such simulators in almost the exact same manner as the device you have, allowing you to see precisely how it functions at all stages of use. You will also have to establish interoperability and manageability at this stage.
- **Product Deployment:** At this point the device must be able to self-register using hardware based security and a unique identity key, among other security features. Once deployment begins, if there are any remaining issues with the device, especially with regard to security, you will have to go back and address them, which is a lengthy and time-consuming process.

One of the biggest challenges in terms of interoperability is protocol translations. Many devices will need to communicate over a wide array of protocols including Ethernet, Wi-Fi, Bluetooth, near field communication, 82.15.4 standard GSK and LTE. Each of these must be secured in its own way, both when communicating within the protocol and transferring data from one to another. Your device must also be able to quickly translate from one protocol to another. This is an area where milliseconds matter.

One of the biggest challenges in terms of interoperability is network connectivity. Many devices will need to communicate over a wide array of wireless technologies including Wi-Fi, Bluetooth, NB-IoT, LoRa, Sigfox, and LTE-M. Each of these technologies would require some similar, some different approaches to security. And, as each of these technologies compete to become the new standard, your device will need to be modular enough to accommodate a different technology as the standard emerges.

When upgrading an existing device to an intelligent device, you can't even assume that the existing components will work properly. For example, adding intelligent components to a functioning "dumb" medical device can mean that you may now have battery issues or heat dispersal issues that were not present in earlier versions of the device. The proof of concept and pilot phase should include testing for these issues so that you do not encounter any later on when you begin production.

Your Internet-connected devices are no good without performance and biometric dating coming from the device. This information then needs to be stored, curated and processed, both on the device and in the cloud in a timely manner to provide meaningful analytics, and alert and reporting capabilities. How you will do all of this is the $64,000 question. It all underscores the importance of taking the time to go through the steps, perhaps most importantly the pilot and business justification.

The Internet of Things and smart medical devices have the potential to revolutionize the medical device industry. However, rollout must be executed properly. Medical device companies need to leverage cutting-edge technologies to provide patients with new levels of care. However, FDA oversight means you have to go the extra mile before you even start developing new technologies. The privacy and security concerns are far from academic. The sensitive nature of the information as well as access to the devices requires a level of security far and above that of any other industry.

Finally, connected medical devices also must have a post market security program in place. Gone are the days of shipping a medical device and leaving it alone, without an automated and controlled method of delivering software updates. After the publication of the "FDA Postmarket Management of Cybersecurity in Medical Devices" in December 2016, SPK developed a post market security platform for a Fortune 500 manufacturer with an associated operating procedure which evaluates, tests, and delivers software updates to connected medical devices.

WWW.SPKAA.COM

Navigating Compliance and Cyber Security Concerns in Smart Medical Devices

visit spkaa.com/contact

Call us 888.310.4540

Visit us at 5011 Scotts Valley Drive, Scotts Valley, CA 95066

SPK and Associates is an information technology services company passionately dedicated to enabling digital transformation of medical device companies. SPK's engineering technology practice is completely focused on fulfilling the specialized needs of research and development and engineering groups in regulated industries. We live and breathe product development, translating our know-how into technical services. The end result is a faster product design calendar and release schedule while simultaneously improving the quality of your product. We partner with medical device companies on IoT initiatives. Let us help you make your product development process more nimble and cost effective while improving the overall quality of the end product.

Steve Kling and Christine (Chris) McHale, formerly of Hewlett-Packard, co-founded SPK and Associates in 1997 with the shared mission of improving engineering processes to save companies time and money.

SPK and Associates