Opportunities and Pitfalls for Connected Medical Devices

Galen Data

1331 Gemini Ave., Suite 300, Houston TX 77058

www.galendata.com

info@galendata.com – 281.404.7234

Introduction

The world is facing a host of challenges in health care including aging populations, rising chronic disease rates, increasing costs and growing demand for affordable, personalized care. These challenges provide opportunities for less expensive innovations that improve quality of care and outcomes. There is a strong emphasis from social care services (CMS, NHS etc.) for value-based programs to improve quality and manage healthcare budgets. Medicare estimates $17 billion is spent each year on avoidable readmissions that can be mitigated with early intervention and better at home care[1].

With the world becoming more and more connected with the adoption of mobile and Internet of Things (IoT) technologies, connected healthcare is poised to provide the platform to solve these challenges. Connected health solutions have been proven to improve clinical efficacy, create new care delivery models, reduce clinical errors, and provide cost savings[2].

However, there are major barriers to adoption concerning cost, cybersecurity and data privacy. This whitepaper explores the opportunities and pitfalls of integrating connectivity into medical devices and how companies can navigate the associated risks.

Opportunities

An ever-increasing number of consumer products leveraging the cloud is making the case for medical device connectivity increasingly self-evident. The Internet of Medical Things (IoMT) allows medical devices to be connected to the cloud and to applications. The cloud is where the information is processed and stored, and the applications allow the user interface. Cloud connected devices can directly benefit the patient and health care providers through improved patient compliance, detecting device failures before they become serious adverse events, and collecting data that can lead to more personalized therapy. Connectivity can help manufacturers monitor the health and status of current devices, help improve and elevate efficacy of future devices, and create new devices or services based on discovered, data-driven opportunities. Cloud connectivity provides an accelerated platform for improving and monitoring health.

Connected medical devices can provide new forms of diagnostic services that may be too resource intensive in a standalone medical device. By making these devices simply a collection vehicle, the cost and ease of manufacturing and compliance can be greatly reduced. Cloud infrastructure allows for the execution of diagnostic algorithms, data storage and analytics. Because data is collected centrally, engineers and researchers can improve diagnostic algorithms over time. Machine learning techniques can be used to comb through this data and identify new patterns that can lead to new products or services. Connected medical devices can also provide portable diagnostics devices that can be used for in home collection and diagnosis. The Scanadu Urine Kit is a great example of such a connected device.

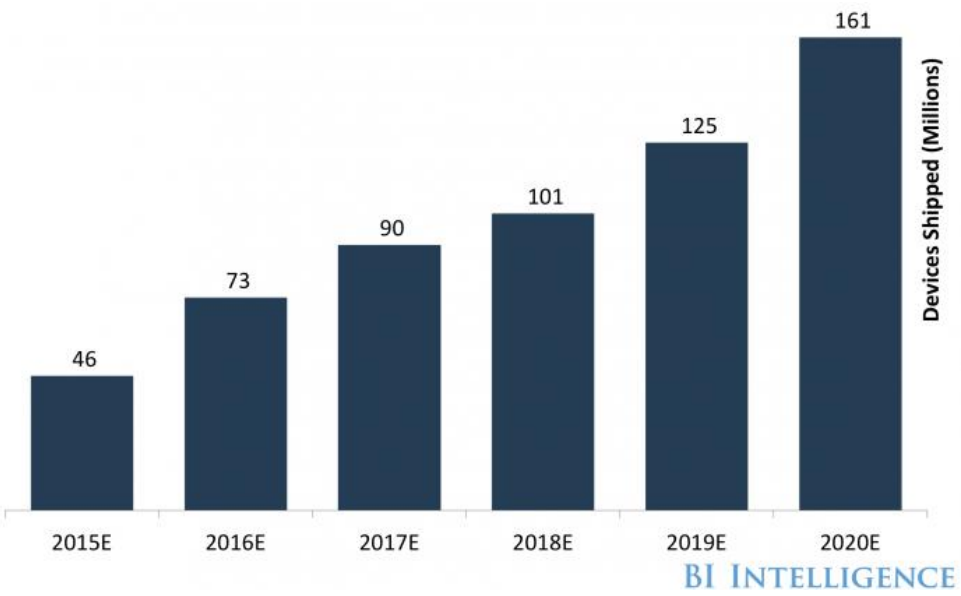
Connectivity can directly benefit both patients and companies. For example, a connected drug delivery device can automatically order refills from the patient's pharmacy proactively. This reduces the risk that patients will run out of critical medication, while at the same time helping companies meet business goals.

Connected medical devices could also help predict potential device failures. As an example, imagine a heart pump manufacturer changed the type of lubricant used for the pump bearings because the original supplier went out of business. The product specification was the same but there was a slight difference in the operating temperature that was not considered an issue. This change resulted in a higher wear pattern on the pump bearings that would go undetected until there was a bearing failure. Instead of having a catastrophic incident in the field, predictive analytics, on the live collected device data, proactively identified perturbations in the pump output. A notification is issued to both the manufacturer and physician, allowing for early intervention and replacement of the soon to malfunction pump and most likely saving the life of the patient and others with the same problematic lubricant.

There is also the "payer" consideration when it comes to compliance. Medicare, for example, requires that for medical device reimbursement, patients must use the device. More and more government regulators and payers are demanding objective evidence that device manufacturers prove their devices are having a positive impact on patient outcomes. A connected medical device can collect and store data about patient use and trace the effectiveness of a particular device and treatment. Connected devices can also help with device traceability and provide ease of software updates when a critical problem is detected in the field.

Additionally, there is a competitive advantage for connected medical devices. Connected medical devices can improve patient engagement, which can lead to higher usage. Increasingly users of medical devices expect personalized services. By connecting a medical device and capturing usage data, customized health information, reminders and alerts can be provided that increase patient engagement with the device. Just-in-time training can be delivered that simplifies usage and can provide more seamless familiarity with the device. Allowing providers to access data remotely at any time, can improve workflows and create new efficiencies for the product team.

In every growing market, a competitive advantage can be a key driver of success. According to PricewaterhouseCoopers, global connected health care will grow to $61B by 2022[3]. Business Insider Intelligence estimates that by 2020 a total of 161 million connected medical devices will be in operations[4].



Connected health provides diagnostic benefits, automated alerts, remote monitoring, improved patient outcomes, and has the potential of lowering the overall healthcare costs. In addition, it opens new opportunities for data aggregation and analysis that can be invaluable for improving existing devices or creating new products and services.

Pitfalls

The two most discussed pitfalls of connectivity are Cybersecurity and Data Privacy. Both are critical concerns for every cloud integrated medical device manufacturer. Connecting devices makes them more vulnerable to both deliberate attacks and undirected malware.

Many recent events, like vulnerabilities found in implantable ICDs and CRT-Ds from St. Jude Medical[5] and the WannaCry ransomware affecting medical devices in the US and UK[6], have demonstrated that cybersecurity is a risk that medical device manufacturers need to manage. The FDA and other regulatory agencies have issued guidelines on managing cybersecurity risk, and the FDA has decided that manufacturers who have streamlined security upgrades on devices don't have to repeat the entire regulatory approval process. Companies will still need to retest and, in some cases, recertify their device. This is a non-trivial burden.

Another concern about connectivity is the cost and expertise required. There is the initial cost of developing a connected solution and an ongoing cost for maintenance, storage and operation of that solution. Often connectivity infrastructure will become an extension of the medical device and must be designed and operated according to the same regulatory requirements as the medical device. In some cases, the connectivity infrastructure itself is the medical device (Software as a Medical Device, SaMD). The expertise to develop and support a connectivity solution that is compliant to FDA and other regulatory requirements is a highly specific skill set not in great abundance.

Solutions

So, can these risks be managed? Absolutely.

As with other aspects of a medical device, a thorough risk analysis should be done to determine the risk posed by connectivity threats. Each medical device has its own risk profile. A heart pump, for example, will have a high risk of patient harm if there is a malfunction, while a blood pressure monitor's direct risk to patient is smaller.

Key points to consider when approaching a connected design are:

1. What is the potential harm to the patient or the operator if data is erased or altered?
2. What kind of data is stored and/or transmitted? Does it include protected health information?
3. What are the business risks of connecting or not connecting a device?

Managing cybersecurity risk requires a detailed plan that encompasses every stage of medical device development, from conception to post market security patches and updates. Some strategies to consider:

1. Create a list of cybersecurity procedures and guidelines. The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework that can be used as a starting point.
2. Train your workforce on good cybersecurity practices. Humans are often the weakest link in cybersecurity defense.
3. Identify, prioritize and track cybersecurity risks as part of product development.
4. Ensure good engineering practices by prioritizing secure design and secure coding throughout the product development and maintenance cycle.
5. Periodically review known vulnerabilities against third-party libraries or with products focused on design or operation of the medical device.
6. Ensure verification includes cybersecurity verification like Penetration Testing, Fuzz Testing and frequent reviews of security controls.
7. Limit the data stored and transmitted to what is essential to the operation of the device or service.
8. Choose the right type and level of encryption. The greater the risk to patients or operators due to altered, deleted or stolen data, the higher the level of encryption used. Always use encryption when transferring data between devices or over a network.
9. Use appropriate security controls for access to data. Enforce password management practices such as length and complexity restrictions, password expiry, the prohibition on reuse of passwords etc. For added security consider a second factor for authentication like a One Time Password, biometric security or security badges.
10. Establish a post-market surveillance program that monitors for newly discovered cybersecurity vulnerabilities and threats. Always conduct assessments, identify mitigating actions and deploy the mitigation after verification of software patches.

Another aspect related to security is data privacy and data export regulations. Both U.S. and global markets have strong data privacy regulations. The Health Insurance Portability and Accountability Act (HIPAA) and subsequent Health Information Technology for Economic and Clinical Health (HITECH) Act establishes standards that need to be implemented for protecting data privacy for all US providers and their business associates. European Union's (EU) General Data Protection Regulation (GDPR) requires strong protection measures for data privacy and addresses export of data outside of the EU. GDPR's protection is much broader than that of HIPAA/HITECH.

Creating a data protection plan that navigates different jurisdictions is essential if the manufacturer wants to sell to the global market. Things to consider are:

1. Identify what data elements, collected or stored by the device, are protected by each set of regulatory standards. Keep in mind that GDPR defines a broader protected set than HIPAA/HITECH.
2. Ensure patient consent is obtained before processing data and keep records of the consent secure.
3. Create data privacy guidelines and ensure your workforce is periodically trained.
4. Create and routinely review audit trails to ensure only authorized users have access to view or alter protected data.
5. Create a program to notify affected users in case of a data breach. Under GDPR the timeline to report any breach is 72 hours from becoming aware of a breach.

Cost of connectivity can also be managed. Cloud based managed services allow for more efficient cost outlay and removes the need of hiring additional personnel to operate and manage the infrastructure. Advances in global connectivity and cloud technology is making cloud-based solutions increasingly attractive for managing cost, while providing superior experience to clinicians and patients.

Conclusion

In conclusion, connectivity for medical devices can be a very beneficial tool for improving the patient health, if risks are identified, monitored and compliance is well understood. In most cases, the benefits — in terms of greater convenience, easier adherence, improved insights, and better health outcomes — far outweigh the risks.

About Galen Data

Galen Data's Galen Cloud is an FDA/HIPAA compliant platform that accelerates medical device cloud connectivity in a fraction of the time and cost it takes currently. FDA Class I, II, III and CE marked medical devices are currently supported. Built under an ISO 13485 compliant Quality Management System, the platform meets or exceeds design control requirements for both US and global markets. Security is actively managed, and tools are provided to comply with data privacy regulations. The platform provides widgets to intuitively present data to Clinicians, Patients and/or their families. Galen Data manages the burden of creating and managing IT infrastructure, so companies can focus on device innovation. The platform is modular and fully scalable. The Galen Cloud is hosting provider agnostic, requires little to no customization and comes with full audit support. The goal of Galen Data is not just to lower the barrier to entry for medical device connectivity, but to open the market to any size device manufacturer.

About the Authors

Chris DuPont
CEO, Galen Data
chris@galendata.com

Chris has over 25 years of experience in designing medical device software for FDA Class I, II and III devices. Chris has led organizations through multiple audits and is expert at Quality Management Systems.

Abbas Dhilawala
CTO, Galen Data
abbas@galendata.com

Abbas has over 13 years of experience developing enterprise grade software for the medical device industry. He is well versed with technology and industry standards regulating security and privacy of data.

Alex Condon
COO, Galen Data
alex@galendata.com

Alex has over 12 years of experience in operations, marketing and business development including bringing innovative products to market in the health care industry.

1. Findings from Recent CMS Research on Medicare, https://kaiserhealthnews.files.wordpress.com/2014/10/brennan.pdf
2. Making the case for connected health, https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_11/Accenture-Making-Case-Connected-Health.pdf
3. The IoT is coming to healthcare, https://www.forbes.com/sites/jonmarkman/2016/09/15/the-iot-is-coming-to-healthcare/#6aa85b022b91
4. The global market for IoT healthcare will top $400 billion in 2022, http://www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5
5. Abbott releases firmware to fix cyber vulnerabilities in cardiac devices, https://www.healthdatamanagement.com/news/abbott-releases-firmware-to-fix-cyber-vulnerabilities-in-cardiac-devices
6. Medical Devices Hit By Ransomware For The First Time In US Hospitals, https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#408c0834425c
7. Threat Report - Connected Medical Devices, https://www.zingbox.com/resources/threat-report/

