The State of Medical Device Cybersecurity

Vidya Murthy and Mike Kijewski[1]

Abstract:

Beginning with breaking down why cybersecurity matters, we discuss the evolution from privacy to patient safety. Considering the regulatory evolution specific to medical device cybersecurity posture over time, we investigate the difference between mandated behavior and better practices portrayed by device vendors. Through an empirical review of healthcare hack events, we explore trends in the types of device vulnerabilities that have led to cyber-events and those which have been researched to have an impact on patient safety. Lastly, we will consider the healthcare community as a whole and reflect on the roles medical device vendors, security researchers, health delivery organizations and service providers play in increasing our collective maturity as well as challenges each function faces.

MEDICAL DEVICE CYBERSECURITY has hyperbolically been portrayed in a Homeland episode where the fictional vice-president's pacemaker is hacked and a Grey's Anatomy episode where the hospital is shut down by a hacker. In reality, the state of cybersecurity in medical devices as part of the healthcare ecosystem is something to be understood in the context of patient care.

The healthcare industry is a complex web of payers, providers, medical device manufacturers, third-party vendors, and (perhaps most importantly) patients. Over the last decade, technology has played a central role in advancing quality of care, creating new delivery mediums and changing access for patients, in large part due to the development of new connected medical devices. The lesser-discussed innovation has been in viewing healthcare cybersecurity as a HIPAA compliance mitigation instead of a patient safety mechanism.

Cybersecurity and patient safety

Frequently perceived as *the* regulatory burden for Healthcare Delivery Organizations (HDOs), device vendors and clinicians, the Health Insurance Portability and Accountability Act

[1] VP of Operations at MedCrypt, vidya@medcrypt.co, 125 South Hwy 101, Suite 101, Solana Beach, CA 92075 (Murthy) and CEO/co-founder of MedCrypt, mike@medcrypt.co, 125 South Hwy 101, Suite 101, Solana Beach, CA 92075 (Kijewski).

(HIPAA) has had an indelible impact on our healthcare system. An average of 35 HIPAA violation complaints (HHS Office of the Secretary, Office for Civil Rights. (2019, May 16) are made on a daily basis with estimates that 59% of the U.S. population has had its health records breached/exposed (HIPAA Journal, n.d.). Since the mandated compliance date of April 2003, the challenge of complying with HIPAA rules has created various cybersecurity programs to control the flow of personal health information.

The introduction of connected medical devices not only expands the scope of HIPAA management, but also introduces patient safety considerations. What if a glucose monitor is manipulated and the attached insulin pump provides an injection that a patient doesn't need? What if a critical calculation in radiation therapy is manipulated? (Chen, Xiao, and Li, 2014). Although Homeland showed a pacemaker vulnerability exploited in an assassination, this is not a common scenario that HDOs and patients face (Homeland, 2018).

A possible attack may include a hacker gaining control of an HDO via a medical device that is compromised. For example, a hacker may access an HDO's network, and inhibit its ability to update electronic health records and use devices that rely on connectivity for delivering care (such as devices used in radiation oncology and sophisticated surgical robots).

While a possible solution may be to revert to pencil and paper during a ransomware attack and rescheduling any elective procedures, delayed operational capabilities can also result in a re-routing of patients who have emergent needs. Extant research documents a 13.3% higher mortality rate for patients experiencing a cardiac arrest who received a delay in care of four minutes (Jena, Mann, Wedlund, and Olenski, 2017). When applying this finding to a delay in care due to a network takeover by hackers, one can imagine an increase in mortality rates far greater than 13.3%.

Regulatory requirements - today and looking forward

Issuing their first guidance document in January 2005, the Food and Drug Administration (FDA) has actively worked to build a collaborative cybersecurity community including clinicians, hackers, device manufactures and HDOs. Most recently the PreMarket and PostMarket Management of Cybersecurity in Medical Device documents have created a clear roadmap and goals for the industry to work towards.

PreMarket Guidance (Food and Drug Administration, 2018) -

While this guidance remains in draft form after its initial released in October 2018, there are a few areas of focus that it will endorse once finalized (expected sometime in 2020):

- Devices should make extensive use of encryption to keep data private.
- Digital signatures should be used to verify authenticity of devices, data and instructions.
- Devices should be designed in a way that anticipates regular, routine cybersecurity patches.
- User authentication needs to be secure and robust.
- Devices should be able to alert users when a cybersecurity breach occurs.

PostMarket Guidance Food and Drug Administration, 2016) -
Released in 2016, this guidance includes a combination of process and procedural requirements for both medical device manufacturers (MDMs) and HDOs. These requirements include:

- Understanding, assessing and monitoring vulnerabilities and risks.
- Implementing robust software lifecycle processes that including having a process for ongoing updates and patches.
- Threat modeling cybersecurity risks around a medical device.
- Participating in a coordinated vulnerability disclosure policy.

The FDA has made it clear that MDMs and HDOs must collaborate to successfully build a robust security program.

Threat sharing as a view to cybersecurity trends

One of the recommendations in the post-market guidance is for device vendors to participate in "threat sharing," in which information about security vulnerabilities is shared with the medical device community via Information Sharing Analysis Organizations (ISAO).

Two of the presumed benefits of threat sharing are that 1) industry stakeholders have the information necessary to minimize their cybersecurity risk and 2) other medical device vendors can use this information to prevent their products from having the same or similar vulnerabilities.

The ICS-CERT Advisory Database plays a critical role in bringing visibility to emerging threats by building a repository for medical device vendors to communicate with each other and customers. Assessing these advisories offers insight into cybersecurity practices in place at various medical device manufacturers. In total, 61 medical device advisories were released between 2013 and February 28, 2019, consisting of a total of 144 cybersecurity vulnerabilities.[2]

Frequency is Increasing

Prior to the Postmarket Guidance (December 2016), advisories were issued at a rate of 0.95 vulnerabilities / month, but subsequent to the guidance release it increased 432% to a rate of 4.11 vulnerabilities / month. A hypothesis presents itself here - has there been an increase in the number of vulnerabilities in devices, or has the FDA guidance which encourages "threat sharing" helped the industry move up the cybersecurity maturity curve?

It is possible that medical device vendors face a perceived stigma when issuing information about security vulnerabilities, and this inhibits participation in this process. Media has certainly picked up advisories and cherry picked attributes from disclosures to highlight security shortcomings. In reality**, disclosing security vulnerabilities indicates a strong and operational security program.** Security is constantly and rapidly evolving. It is not a 'one and done' activity, but instead must be doggedly managed, which means ongoing vulnerability identification, disclosure and remediation. As other device vendors mature their programs, another 4x increase in the rate of disclosure can be anticipated.

[2] Raw data available at https://docs.google.com/spreadsheets/d/1GDIN_BAdHndK3TvzbWZUCnC09xqJrqe-uxEoCxBVc5U/edit?usp=sharing.

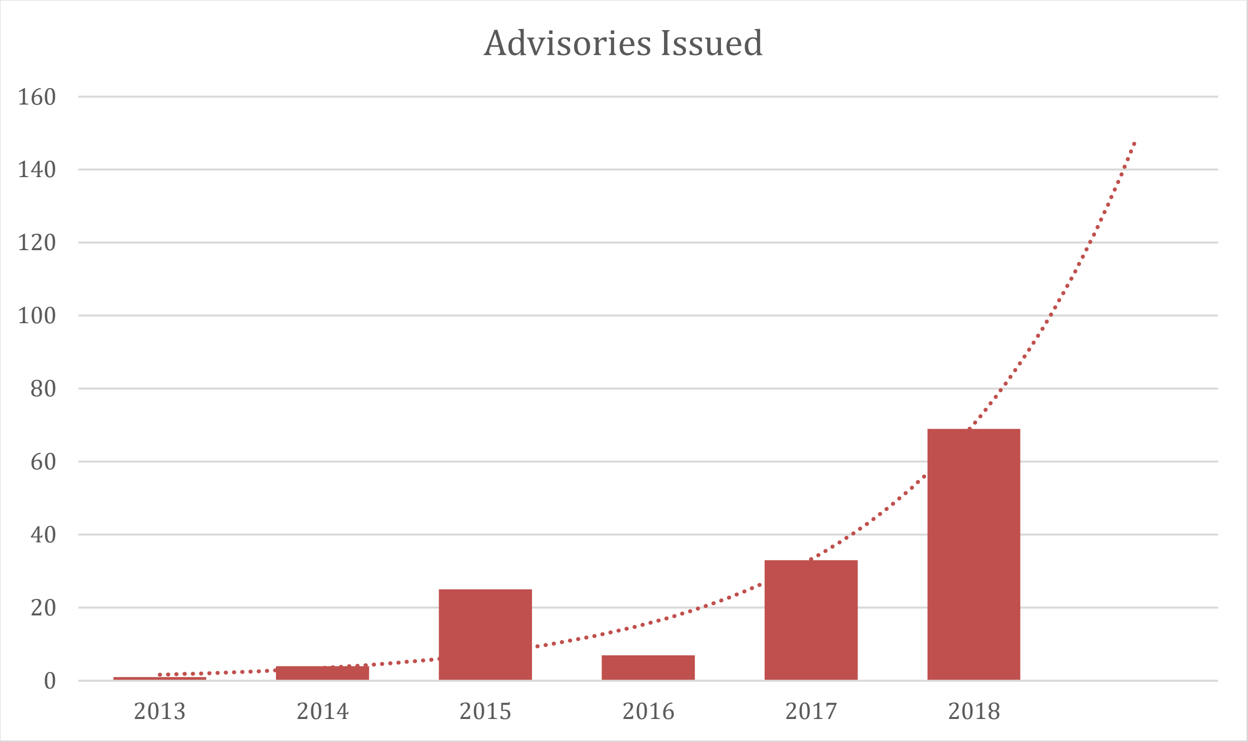

Figure 1

Some Companies Have Yet to Issue an Advisory

A comparison of the list of companies who have made disclosures, against a list of connected-device vendors ranked by market cap, shows that only ten (10) of the top twenty nine (29) medical device vendors have ever made a vulnerability disclosure through ICS-CERT. That leaves 19 top medical technology vendors that have never made a disclosure. It is highly unlikely that there are no security vulnerabilities in any of the devices they currently sell.

There are two valid reasons a medical device vendor would never have made a disclosure.

1) Their devices have no vulnerabilities.
2) They have never been made aware of or discovered a vulnerability.

Vendors who have not issued an advisory should continue to ensure their product development lifecycle aligns with the requirements outlined in the FDA pre- and post- market guidance. These vendors should also consider partnering with the security community, perhaps in the form of a bug bounty program, to ensure rigorous security practices (Bugcrowd, 2019).

Noting that 36.84% of all advisories were disclosed by two companies (Phillips and Becton, Dickinson), there is perhaps a hypothesis here between size or organization and frequency of disclosure. The FDA draft pre-market guidance (October 2018) proposes a tiered structure to align security requirements with impact on patient safety, but does not change requirements based on the size of company.

Certain Classes of Devices are Under-represented

There are certain classes of medical devices that are absent from ICS-CERT advisories. One expects a uniform cross section of the networked medical device market, yet the advisories tend to focus on specific device classes, like pacemakers, insulin and infusion pumps, and imaging systems.

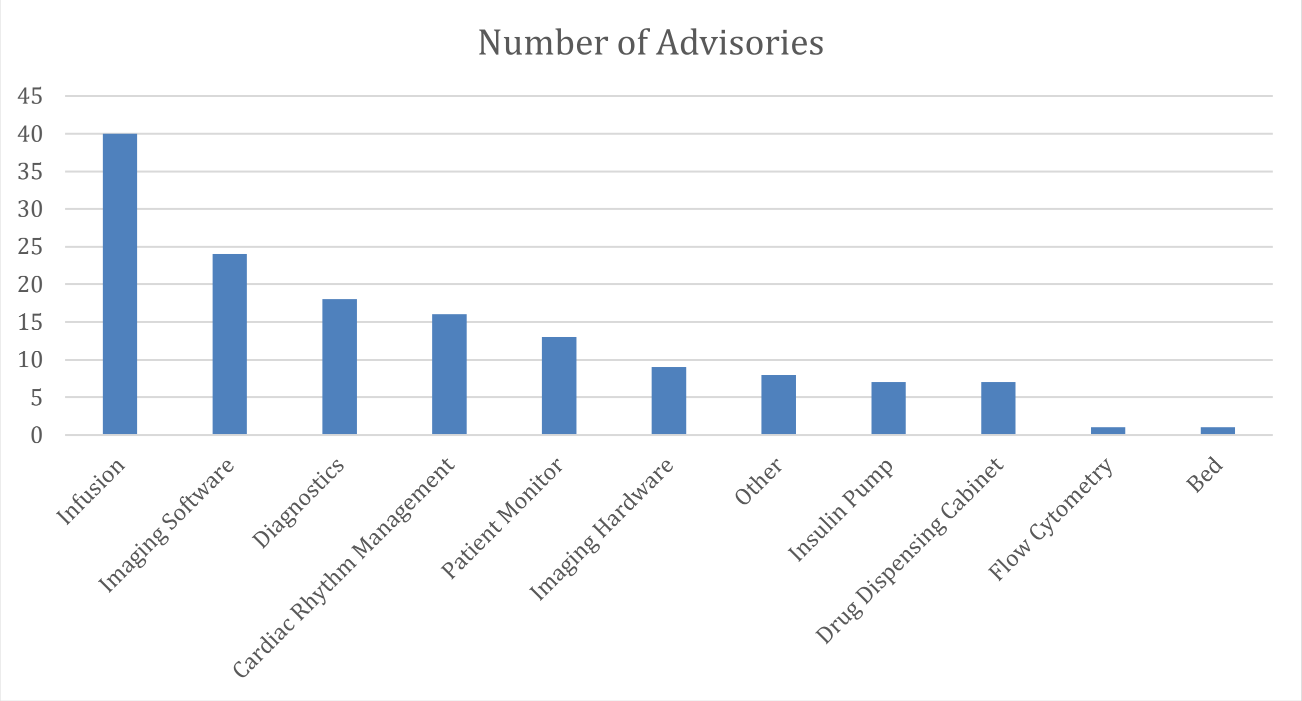

Figure 2

It seems unlikely that a certain class of device is any more or less vulnerable than another class of device. Cybersecurity researchers are directly cited in 43% of all vulnerabilities to date – and noticeably absent from any of the imaging software advisories. Could it be the device classes with advisories are attributed to these devices being more accessible to security researchers?

Issues with User Authentication is a Common Problem

Vulnerabilities attributed to user authentication and code defects covered 66% of all vulnerabilities. Is it possible that user authentication is the most commonly reported on because it is the first thing a penetration tester would interact with? If that is true, future advisories are likely to focus on deeper “layers” of the technology stack as medical device cybersecurity matures. In comparison, advisories from the more cyber-mature industrial control systems (ICS) industry demonstrate a variety of custom developed attacks and multi-pronged strategies that have to work together to successfully a vulnerability.

Patient Impact

A common rebuttal targeting the efficacy of cybersecurity efforts in medical devices is the absence of a death attributed to a cybersecurity event. Perhaps the question to be asked is why is it so difficult to track this statistic. Attributing a medical device cybersecurity incident to the loss of a life is incredibly difficult due to the limited logging capability of devices, missing attribution data and a lack of historical regulatory requirement.

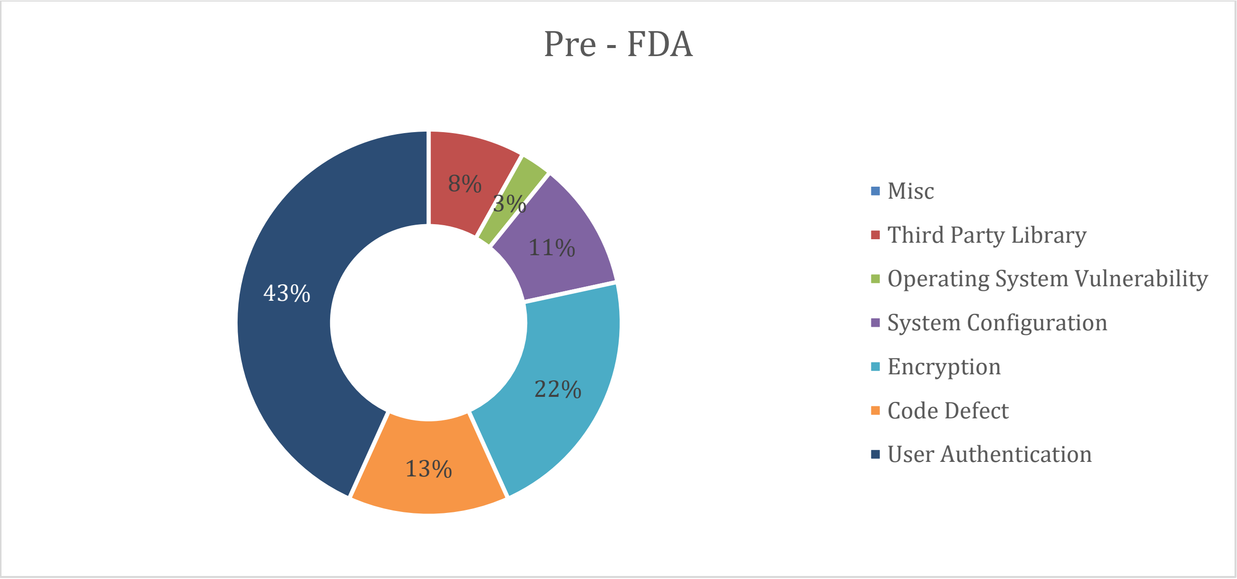

Figure 3

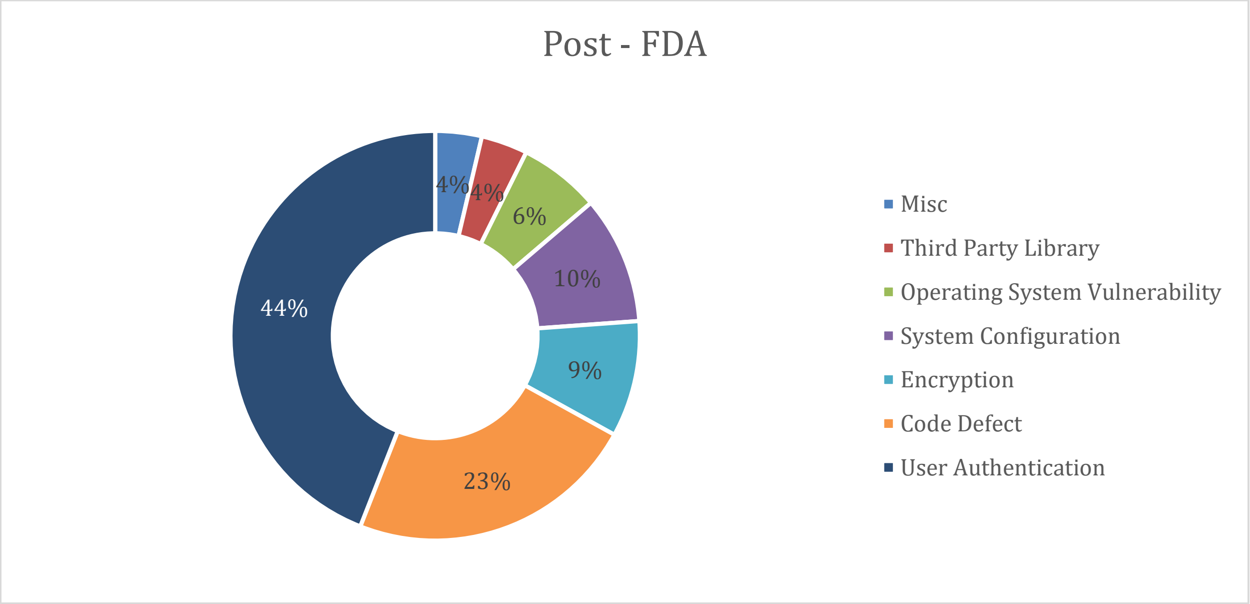

Figure 4

In 2016 when the FDA released their post-market cybersecurity guidance, it mandated device log management and analysis. This indicates that at a future date, we should have technical insight to assess the impact of device information integrity on clinical outcomes. It also indicates that at this time, many ‘live’ devices were never designed to capture log data.

Attempting to capture data that is currently available, the Safe Medical Devices Act of 1990 created the Manufacturer and User Facility Device Experience (MAUDE) database to capture device-related fatalities and adverse events for both device manufacturers and the FDA. Manufacturers are mandated to report any adverse event communicated to them.

The table below captures the problem types determined to possibly originate from a cybersecurity problem, with the related number of reports.[3]

Problem Type	**Number of Reports**
Application Program Version or Upgrade Problem	95
Application Security Problem	1
Computer System Security Problem	13
Patient Data Problem	788
Problem with Software Installation	259
Unauthorized Access to computer system	37

Table 1

In total, 1,193 unique MAUDE entries from January 2010 - February 28, 2019 were found for the selected problem types.

An additional search for 'cybersecurity' in the "advanced search" interface identified 244 reports. However, this was across only three companies: Roche, Siemens and St. Jude. With 229 of the MAUDE entries coming from St. Jude, the absence of diversity in vendors makes it difficult to conclude about trends in reporting, but does validate the challenge in obtaining data from events that result in physical harm (or even death) due to cybersecurity vulnerabilities.

In reviewing these MAUDE entries, there is an absence of technical data, making it difficult to assess incidents from a technical perspective and determine how a cyber threat resulted in a problem that caused a loss of life.

Looking Ahead

The lack of details that are captured when issues arise is the result of log retrieval not being architected into a device. The lack of this fundamental security feature could be the result of several factors, including:

- The high volume and variety of devices deployed means the type of information retrieved can vary significantly in utility for forensic review.
- Since devices operate in a variety of settings, such as hospital networks or with limited wireless connectivity, accessibility to retrieve history can be unpredictable.
- Depending on the memory available on a medical device, there may be a limit on the history it retains.

Complicated hospital IT infrastructures can cause the device's interactive interface to only provide limited information to be available for review.

We think medical device vendors have been making lots of progress over the last few years and we have yet to see a case where the cybersecurity of a device outweighs its clinical benefit. With the FDA's encouragement the market is starting to understand that vulnerability disclosures are indicative of a working security program. We predict that with the perceived stigma associated with disclosures waning, additional device classes & companies to will start disclosing

[3] Raw data available at (requires a request for access): https://drive.google.com/open?id=1fuxAhUStUeAv68JKH8SgnV9OfChBYMkdYl4wn4KmB9I

vulnerabilities. Further, we predict that the complexity of vulnerabilities disclosed will also increase. The 400% increase in disclosure frequency to date indicates more device vendors are prioritizing cybersecurity and have functioning security processes.

The FDA premarket guidance goes a long way to outline the roles that different community members will have to play to enhance the collective cybersecurity posture faced by healthcare . With a shared burden it is expected that HDOs will build a more robust practice that considers cybersecurity risk in device design and implementation, and medical device manufacturers will increasingly harden the security of the devices they provide in order to obtain their 510(k).

References

Anupam B. Jena, M.D., Ph.D., N. Clay Mann, Ph.D., Leia N. Wedlund, and Andrew Olenski, B.S (2017). "Delays in Emergency Care and Mortality during Major U.S. Marathons | NEJM." *New England Journal of Medicine* 376, 1441-1450.

"Broken Hearts (Homeland)." *Wikipedia*, Wikimedia Foundation, 9 Sept. 2018, en.wikipedia.org/wiki/Broken_Hearts_(Homeland).

"Bug Bounty List." *Bugcrowd*, www.bugcrowd.com/bug-bounty-list/.

Chen, W., Y. Xiao, and J. Li, 2014. Impact of dose calculation algorithm on radiation therapy, *World Journal of Radiology* 6, 874-880.

Food and Drug Administration. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff*. Available at: www.fda.gov/media/119933/download. Accessed June 13, 2019.

Food and Drug Administration. *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. Accessed June 13, 2019.

Healthcare Data Breach Statistics. (n.d.). Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

HHS Office of the Secretary, Office for Civil Rights. (2019, May 16). Enforcement Highlights - Current. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html