Note: the following is just starting to become a major issue for device manufactures, however, in the future, sadly it will greater.

**What Outdated Medical Devices Mean for a Network — and How to Protect Yours**

It’s not just phishing emails and rogue links that are putting your healthcare organization’s network at risk.

*by Susan Hall*

Susan Hall spent more than 20 years as a newspaper writer and editor in Dallas and Seattle before making the leap online at MSNBC. Now living in Louisville, Kentucky, she has focused on enterprise technology. Despite an understanding in the healthcare community that unsecure and legacy medical devices are particularly susceptible to cyber attacks, that concern hasn’t necessarily translated into action.

Case in point is a survey released by the Ponemon Institute, which found that 67 percent of medical device manufacturers and 56 percent of healthcare delivery organizations believe an attack on a medical device built or in use by their organization is likely to occur in the next year. But only 17 percent of device makers and 15 percent of healthcare organizations are taking significant steps to prevent attacks.

Moreover, only 51 percent of device makers and 44 percent of healthcare organizations follow current Food and Drug Administration guidance to mitigate or reduce inherent security risks in medical devices, according to the study.

“The lackadaisical approach that [health organizations] take, for the most part, is the reason they’re so vulnerable. The treasure trove of electronic health records PII [personally identifiable information] is ready to be taken with very minimal acumen by the actual adversary,” says James Scott, senior fellow at the Institute for Critical Infrastructure Technology (ICIT).

Cybersecurity Collaboration and Leadership Are Key

Too many hospitals depend on their IT departments to also fill the role of cybersecurity experts, Scott says. But the IT departments don’t always have the training and understanding of what’s necessary to develop and maintain a strong cyber defense.

On the other hand, organizations with a senior information security leaders are more likely to adopt a holistic approach to cybersecurity, according to the 2017 HIMSS Cybersecurity Survey.

“Most of these [small] organizations don’t have CISOs. They don’t have cyber-centric experts on the board or even advising them,” Scott says. “If you don’t have qualified people to put this together, if you don’t have qualified people to listen to the vendors’ pitches, you don’t know how to buy, you don’t know how to layer your security measures.”

Often, even when there is a dedicated security team in place, they aren’t properly consulted on each new device joining the network.

At the University of Vermont Health Network, for example, the six-hospital network makes security part of vendor vetting — it just upgraded around 700 infusion pumps — but occasionally security pros learn of machines expected to go on the network the day it arrives.

“Somebody bought it, signed a contract for it and the information security department was never told about it,” says Richard Schaaf, regional information security officer for the University of Vermont Health Network. “Our only option at that point is to use some technical network mechanism and work with a clinic, take a look at their workflow,” he says, adding that the tech could be adjusted to add an extra layer of security to ensure patient safety.

Guidelines Seek to Close the Legacy Device Security Gap

A main issue, according to Schaaf, is that buying newer models does not mean they are more secure. FDA guidance on medical devices tells manufacturers they have an obligation to consider the cybersecurity of their devices during design and throughout the operating life of that device, though the FDA’s follow-through on that remains a mixed bag.

“The problem is we’re chasing security after-the-fact,” says Schaaf, who also calls using the network to secure devices “putting a Band-Aid on something that needs to be healed.”

For the Department of Health and Human Services’ Cyber Security Task Force, legacy medical device cybersecurity is a major concern, and one that took center stage in its latest report. The task force called for developing incentives for organizations to replace lega-
cy devices that are particularly vulnerable to an attack, such as a “Cash for Clunkers” program.

According to the FDA, medical devices should be considered a hostile environment for hacking and devices have to be hardened against it.

System-level security is a shared responsibility, according to the cybersecurity principles released by Advamed, a digital health trade group. The guidelines call on device makers to work with healthcare organizations after the sale to ensure devices work as intended to protect patients and systems.

Future Policies Promise to Push Device Security to the Forefront

At the federal level, two device security bills have been proposed. The Medical Device Cybersecurity Act of 2017 would create a “cyber report card” to increase transparency of medical device security. The Internet of Medical Things Resilience Partnership Act calls on the FDA to set up a public-private working group to “develop recommendations for voluntary frameworks and guidelines.”

Scott, however, maintains that the industry cannot police itself, and points to three efforts that could make a big difference:

• The Department of Health and Human Services launched the Healthcare Cybersecurity and Communications Integration Center (HCCIC) earlier this year, an intelligence-sharing clearinghouse for coordination between the healthcare sector and the Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC). It aims to provide real-time communications among incident response teams. ICIT calls this a major step forward in introducing real cybersecurity resiliency and moving healthcare organizations away from self-regulating, checkbox-driven security standards. Scott characterizes this effort as stalled.

• The Cyber Shield Act would create an Energy Star-type program to provide buyers with more specific information about medical devices. It would require security-by-design throughout the development lifecycle in accordance with National Institute of Standards and Technology (NIST) 800-160, which addresses how to develop secure systems from the bottom up.

• A more aggressive push toward NIST standards.

“There’s a lot of talk, and that’s all it is — talk,” Scott said. “Why don’t we deal with the plethora of [proposals] already on the table? Let’s move forward, let’s just start.”

How Organizations Can Keep Medical Devices Safe

In the meantime, how can manufacturers and IT teams work together to understand a device’s vulnerabilities? It’s vital for organizations to understand how each device treats a patient as well as the information it collects and where that information resides, says John Fowler, deputy information security officer for the Henry Ford Health System in Detroit. He encourages organizations to ask where medical data from the device is stored, whether on the device itself or a central console.

Many devices are mobile and use wireless connections, which is where employing encryption to keep medical data safe as it moves from one device to another is critical.

Lately, organizations have also started looking at network segmentation, he says, because there’s a cost to it, and organizations generally like to have a flat network for accessibility.

“The next generation of firewalls actually provides that [segmentation]. You don’t have to build out a specific infrastructure; now I’m creating a bubble within my network for medical devices,” Fowler says, adding that the cost of segmentation is dropping significantly.

Many security pros consider automation, such as machine-to-machine learning and artificial intelligence, as the best option.

“The speed of today’s security environment means that if a human is involved, an event will have moved past [network] security and is now a forensics case,” Robert Kingma, CEO at ICT Networks told IT chiefs gathered in Sydney recently, according to CIO.

Many security vendors reject the perimeter firewall approach to security, because once it’s breached, malicious actors can freely move through the network. Instead, vendors use machine learning to determine normal behavior of systems and monitor and alert in near-real time on aberrations. They also call on combined community knowledge in cloud-based analytics engines to parse true problems from noise.

Using automated software to find unknown open ports, default credentials, missing patches, bad code and known vulnerabilities across enterprise systems can be invaluable, but such systems have yet to gain widespread traction within healthcare.

“The jury’s still out on whether that kind of technology will be helpful,” says Schaaf. 😊

When Is Digital Technology Not a Medical Device in the US?

Eager to offer a digital health technology, but not as excited about being labeled a medical device by FDA? This must-know information is vital for companies hoping to confirm that a product is not a medical device.
FDA has an impressive collection of ongoing digital health initiatives, and the regulation of software and hardware has evolved greatly since smartphones and tablets were launched about a decade ago. In FDA’s recent overview of its initiatives, the “Digital Health Innovation Action Plan,” the agency states, “From mobile medical apps and fitness trackers, to software that supports the clinical decisions doctors make every day, digital technology has been driving a revolution in health care.” No one would argue with them on that, and it is difficult to imagine a medical institution that hasn’t adopted smartphones and tablets for daily clinical and administrative uses.

While “a revolution in health care” sounds exciting for end users, it’s less exciting to consider whether a particular healthcare IT product is subject to federal regulation because it meets FDA’s definition of a Class I (low risk), Class II (medium risk), or Class III (high risk) medical device. On that issue, the audience typically falls into three groups, which I’ll call the “incumbents,” the “contenders,” and the “hopefuls.”

The incumbents are existing medical device manufacturers (think GE Healthcare) with experience obtaining 510(k)s or PMAs for hardware and software devices. The contenders (think Samsung) are companies that do not historically have such experience, but have decided, for business reasons, to enter the regulated medical device space, including filing 510(k)s, implementing a quality system, etc. As for the hopefuls, they prefer to remain outside FDA’s jurisdiction, so they ask a simple question: How do I confirm my product is not a medical device?

The general answer is that the product needs to fall into one of five buckets set forth in Section 3060 of the 21st Century Cures Act (Cures Act), which include certain software that: 1st supports administrative functions of a healthcare facility, including population health management; 2nd encourages a healthy lifestyle (and is “unrelated” to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition); 3rd serves as electronic patient records, including patient-provided information; 4th assists in displaying or storing data (i.e., a “Medical Device Data System”); or 5th provides limited clinical decision support (excluding imaging).

Now, before anyone in our “hopefuls” group gets too hopeful, these bullets are a high-level overview of eight pages of statutory language from the Cures Act, and “certain software” does not mean “all software.” As Congress warned, “[s]oftware remains subject to regulation as a medical device if: (1) the software acquires, processes, analyzes, or interprets medical information; or (2) the FDA identifies use of the software as reasonably likely to have serious adverse health consequences.”

So now that you see the areas of opportunity and a Congressional reminder on what to avoid, you need to select a category that most closely matches your technology and get to the next level of detail to hopefully confirm that you are squarely within an exemption. For the first four groups, including mobile apps, chances are good that FDA has clarified things, perhaps through one of the guidance documents or regulations they have issued in this area within the last several years.¹

For example, if you have a cloud-based iOS/Android healthcare app and you’d like some assurance that FDA will not consider it to be a regulated “mobile medical app,” you could peruse the 45-page FDA guidance on the subject that includes nearly 30 examples. You may find a kindred spirit in the apps described where FDA has said, in effect, “even if these fall within the definition of mobile medical app, we are choosing not to regulate them.” Some “hopefuls” may find the analysis ends there on a happy note.

Clinical Decision Support Software

But what about that last category—Clinical Decision Support—and why does FDA call it “limited” CDS and not just CDS? Although CDS has been under discussion for years, FDA has never issued guidance on it, while other categories, such as medical device data systems (MDDS), have been the subject of one or more guidance documents. Now that the Cures Act is live, FDA has an ambitious goal of quickly issuing several new medical device guidance documents, including a draft guidance by the end of 2017 that speaks to the effect of the Cures Act on previous guidance documents—the section on mobile apps should be interesting—and one on CDS by March 2018.

Therefore, of the five exemptions listed above, the probability of industry interpreting things differently than FDA is fairly high with CDS, but less so for the others. While that alone is not a reason to delay launching a promising CDS product, the last thing a “hopeful” wants to hear is that the FDA views them as a “contender.”

Software Designs with FDA Implications

So other than looking into a crystal ball, is there anything a software development team can do to better understand the elements that would make it more or less likely that someone at CDRH will view a product as falling outside all five buckets? Maybe. There are at least two software concepts that have significant FDA implications: 1st Passive versus active Supplemental versus primary

The first one is fairly intuitive. It’s the difference between software that handles pre-existing data without substantively changing it, and software that controls a medical device or raises patient safety issues because it invites clinicians to rely on or act upon some patient-specific analysis or interpretation, which, in turn, could affect treatment and diagnosis. If software does something “active,” it’s more likely to be regulated.

When FDA talks about this distinction, they don’t use the term “passive,” but they do speak of “active patient monitoring,” as something that they intend to regulate, because a device that is active in this sense is one “that is intended to be relied upon in deciding to take immediate clinical action.” For example, in the definition of a Medical Device Data System, the FDA expressly excluded “devices intended to be used in connection with active patient monitoring.” In the MDDS guidance, FDA provides a few examples, such as an app that conveys data from a blood glucose meter. It’s “active patient monitoring” if the software is intended to alert a caregiver to take immediate clinical action. On the other hand, it’s not “active patient monitoring” if the software “facilitates the remote display of information from a blood glucose meter.
where the user of the meter can independently review their glucose and glucose levels, and which is not intended to be used for taking immediate clinical action.”

The mobile medical apps guidance included a similar reference to “active patient monitoring” where FDA cites three examples of regulated software, including mobile apps that: i) connect to bedside (or cardiac) monitors . . . for display and active patient monitoring; ii) connect to a perinatal monitoring system and transfer uterine contraction and fetal heart rate data . . . for remote monitoring of labor progress; or iii) are intended to display images for diagnostic review.”

The second concept—supplemental versus primary—is less intuitive, but think of three levels of software: one that simply displays data, one that highlights certain aspects of the data, and one that suggests a clinical conclusion or decision. Consider an imaging example, where the first is a standard radiology workstation package that allows users to visualize a CT scan of the lungs, the second applies a pattern recognition algorithm and points out specific items within that scan (e.g., lung nodules), and the third provides a probability of malignancy. The first is the base technology, the second is supplemental, and the last one is primary, meaning it’s starting to sound like a treatment recommendation that is ultimately the clinician’s responsibility, as opposed to a tool that helps clinicians decide on treatment.

An Analogy from Imaging—CAD

The FDA uses the term “Computer-Aided Detection”—a Class II device— for the second category (supplemental), which they define as “computerized systems that . . . are intended to . . . direct attention to portions of an image, or aspects of radiology device data, that may reveal abnormalities during interpretation of patient radiology images or patient radiology device data by the [clinician].” The last category is Computed-Aided Diagnosis—a Class III device—which FDA defines as devices that “provide an assessment of disease or other conditions in terms of the likelihood of the presence or absence of disease, or are intended to specify disease type (i.e., specific diagnosis or differential diagnosis), severity, stage, or intervention recommended.” It’s clear that that category will always be regulated by FDA. So, bringing this all back to the five “this-is-not-a-medical-device” categories, software that is “passive” and “supplemental” is likely to be MDDS or CDS. In the case of CDS, the Cures Act excludes from the definition of medical devices software that is intended for the purpose of “supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition,” but only where it also enables the clinician to “independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.” In short, the software has to be supplemental and not primary.

But you may see the conundrum that has been created. Clinical Decision Support software won’t have much value if clinicians see it as merely confirming what they already know, as may be the case with CDS provided to the nation’s leading academic medical centers. The more likely customers of CDS are the community/rural hospitals where modest clinical resources are precisely what makes the software so helpful, and those users are less likely to touch the button that says, “press here to independently review the basis for the recommendation provided.”

If a company markets CDS as the equivalent of having a highly-trained clinician sitting next to you, making thoughtful recommendations that you can rely on, you can expect FDA to classify the product as a regulated Class II or Class III medical device. The agency may want to create a CAD-like set of requirements for your product, including full review of:

- “the algorithm design and function,
- processing steps,
- features,
- models and classifiers,
- training paradigm,
- databases,
- reference standard, and
- scoring methodology”

The fact that the Cures Act created five categories of things that are not medical devices is a really big deal. For “hopefuls” awaiting FDA guidance, you are far better off with FDA’s starting point being a federal statute that says some software is not a medical device rather than the situation a few years ago, where FDA had the power to declare CDS as a Class III device. Another point to remember is that the trends are in favor of the “hopefuls.” To appreciate that, I’d like to turn the clock back to 2011 and highlight one or two vignettes from each of our segments: incumbents, contenders, and hopefuls.

Compare Healthcare Apps Six Years Ago to Today

Let’s say it’s 2011, and everyone is buying Apple’s newest device, the 1st-generation iPad. Many radiologists (but not all) wanted to use them to review images and software professionals wrote programs to make DICOM images show up on iPads.

**Incumbents**

MIM software, a smaller but brave medical imaging software company with years of experience, was already trying to obtain 510(k) clearance for an iOS app that provided wireless access to medical images. After two “non-substantially equivalent” findings (i.e., FDA rejections), the company was told by FDA that their device may be Class III because there is no predicate for mobile viewing capability on a tablet. I’m not sure if the company pursued de novo after that, but it eventually obtained clearance for the first iPad app of its kind. How? The company agreed that their software was supplemental and not primary.

Specifically, the indications for use of “Mobile MIM” included a statement that the “device is not intended to replace full workstations and should be used only when there is no access to a workstation.” While it’s difficult to imagine a situation where a clinician really has “no access” to a workstation, the solution was creative.

GE Healthcare, along with other incumbents, followed quickly with similar products, but were forced to include an alternate version of the “supplemental and not primary” concept, as, for example, the clearance for a cardiac iPad app stated that it “is intended to assist trained professionals in the viewing, analysis, and diagnostic interpretation of images and other information.” Of course, EMR-related apps were launched as well.

**Contenders**

Microsoft obtained 510(k) clearance for software called “Amalga Image Processing Module (IPM),” which was part of an existing software package that was designed to consolidate “disparate health information” with DICOM im-
ages. They, too, were asked to include “supplemental versus primary” language as the indications for use state that it “is not intended to be used for primary diagnosis.”

Hopefuls

In the 2010–2012 range, Apple, Google, and Samsung were not in the medical device space, although they were probably thinking about it.

A startup company named ONKÖL™ was in the process of developing a wireless home-use talking device that could connect to other devices such as a blood pressure cuff or glucometer, remind Mom to take her medication, and send the information to family members’ phones, including the blood pressure or glucometer data, along with confirmation that Mom took her meds. However, if ONKÖL™ had launched their MDDS device before 2011, FDA would have said it was a Class III device that required a clinical trial, as it wasn’t until February of 2011 that FDA “down-classified” MDDS from Class III to Class I. Think about that for a moment—about six years ago, MDDS was a Class III device, even “riskier” than the Class II devices to which it could connect.

Now let’s come back to 2017.

Incumbents

MIM Software’s latest “thin client” is still a Class II device, but with vastly expanded capabilities that operate on iPad, Microsoft Surface, Amazon Kindle, and Samsung Galaxy. While the language about using it only when there is “no access to a workstation” is still there, the scope has been reduced to times when the application is “used for diagnostic purposes.” That makes sense. GE Healthcare has similar follow-on offerings.

Contenders

Microsoft may have decided to become a “hopeful” as they handed “Amalga” over to GE Healthcare, who bundled it into their Caradigm offering.

However, Apple, Samsung, and Google (through their Verily subsidiary) moved from hopefuls to contenders, and all three were among the 9 finalists chosen (from 100+ applicants) as pilot participants for a software-as-a-medical-device “precertification” program recently launched by FDA. Under the “precert” program, reduced pre-market requirements could be applied to companies whose product development and quality systems have been deemed by FDA to “consistently and reliably” deliver “high-quality software design and testing (validation),” including ongoing product maintenance.

Hopefuls

ONKÖL™ has launched their device, and the regulatory timing couldn’t have been better. In addition to down-classifying MDDS from Class III to Class I, and in addition to FDA’s guidance saying that they do not intend to regulate MDDS, the Cures Act has now said that MDDS is not a medical device at all. By not having to deal with FDA issues, the MDDS classification was likely a major benefit for ONKÖL™ in terms of keeping costs down, accelerating the launch, and reaching as many families as possible.

Conclusion

Whether you are an incumbent, a contender, or a hopeful, the direction of FDA regulation in this area is positive. Since the first iPad was launched, several types of healthcare software have moved from regulated to not regulated, and FDA’s guidance documents confirm that they intend to focus their enforcement resources on high-risk software products. If companies design their products in ways such that they are fairly described as not “active” or not “primary,” then the five “non-medical device” categories of the Cures Act will become the standard way to consciously and lawfully avoid FDA regulation. This includes medical device data systems and mobile health apps.

For those developing Clinical Decision Support software, the situation has improved with the Cures Act, but it’s not yet settled, at least until FDA releases CDS guidance, hopefully in 2018. While I’m guessing that FDA may want to pull in rules like those from Computer-Aided Detection in imaging and apply them to higher-risk CDS products, I hope I’m wrong.

In the US we will celebrate a national holiday, which is all good because it includes eating really good food.

Sorry about being a bit let this month.

In case you have not noticed 2017 is just about gone. Get ready for 2018 that will bring a number of new challenges to medical device manufactures.