Division of Dockets Management (HFA-305)

Food and Drug Administration
Department of Health and Human Services
5630 Fishers Lane, rm 1061
Rockville, MD 20852

March 18, 2019

Ref: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
(Docket No. FDA-2018-D-3443-0001)

Dear Sir/Madam:

This is to submit comments on the Contents of Premarket Submissions for Management of Cybersecurity in Medical Devices, as requested by the Food and Drug Administration (FDA) through the Request for Comments issued on 10/22/2018.

Comments

Medical device cybersecurity is a shared responsibility among health systems, independent security researchers, users, and medical device manufacturers. Although FDA's approach in trying to help refine this eco-system and ability to assist the healthcare delivery organization's and the healthcare technology management (HTM) community is impressive, the broader concern is that aspects outlined in the 2018 Guidance Document for Pre-Market Submissions for Cybersecurity are not mandatory. Medical device manufacturers, distributors, and suppliers that are active members of the information sharing and analysis organizations (ISAOs) and active members of the broader cybersecurity discussions respect and follow the recommendations. This is evident from their coordinated activities to support medical devices without strong security controls with the users, i.e., health systems and private practices.
However, there is still a large percentage of medical device manufacturers that, in no way, collaborate, communicate, or coordinate cybersecurity activities with users. That is a big concern for the HTM community, which the American College of Clinical Engineering (ACCE) represents. The ACCE Task Force consists of healthcare technology management/ clinical engineering professionals from health systems of various sizes and independent service organizations. The Task Force attended the January 2019 FDA Workshop that discussed the 2018 Guidance Document for Pre-Market Submissions for Cybersecurity and has compiled the viewpoints of the HTM/ CE community.

Software/ Cybersecurity Bill of Materials (SBOM/ CBOM)

The SBOM/ CBOM are great documents to receive from the medical device manufacturers and is proven to be effective in assisting the healthcare delivery organizations (HDOs) make informed decisions about the medical devices that are purchased and used for patient care. The concern here is

that not all HDOs are equipped with tools to put this document into much use. Majority of the HDOs do not have the capability to track their assets on a software component level basis. Currently, majority of the HDOs do not even document a comprehensive medical device inventory or its information technology (IT) attributes, such as, operating system version, software revision levels, SQL version, Adobe version, IE version, etc.

Transparency in terms of open source and commercial software components that make up the medical device are important for HDOs to prepare during purchasing and installation. This will aid the HDOs to better understand how the software works and how to manage the risk should a vulnerability be exploited. For example, if the SBOM/ CBOM were to be included in the service manual, a technician will be able to troubleshoot common problems and will also gather the understanding on management and timely remediation of a risk. Couple of problems with service manuals is that they are revision sensitive and there is still a wide variance in the industry on what even constitutes a service manual. This lack of standardization creates a problem when acquiring SBOM/ CBOM documents.

If the FDA mandates that medical device manufacturers will support and provide documentation for devices at least every 365 days and that all versions will be available on the manufacturers' website, that will be a big win for the HTM/ CE community.

Several practical challenges in making the SBOM/ CBOM usable are outlined below:

- How to effectively manage the acquisition and use of SBOMs/ CBOMs,
- Roles and responsibilities managing SBOMs/ CBOMs in the HDOs, i.e., will they be tagged with each asset in the computerized maintenance management system (CMMS) and managed by the HTM personnel like the current practice with managing the MDS2 documents?
- Will the HDOs acquire SBOM/ CBOM during procurement? And how they do seek them for existing assets?
- Will the SBOM/ CBOM will be updated and provided to HDOs when the medical device software is updated or upgraded?
- Will the SBOM/ CBOM be publicly available or through a secure vendor web portal?
- Is there a standard format for the SBOM/ CBOM? What are the mandatory aspects that must be outlined in them?
- Will clear use cases be outlined as part of the document so HDOs can readily use them?
- Will the information outlined in the SBOM/ CBOM be specific to each modality or device or the type of configuration deployed in the HDO?

Medical Device Patch Management

The 2018 Guidance Document for Pre-Market Submissions for Cybersecurity calls for anticipation of patches and updates to address concerns and to facilitate rapid verification, validation, testing, and deployment of patches and updates. We do not think that the medical device manufacturer (MDM) will ever allow MS/ AV patches without validating and verification (V&V) for the overall safety of the medical device and its user. Even if there is a requirement or mandate around applying these patches without MDM approval, there will not be enough support from the MDM community. Additionally, guidance should be provided from the manufacturers for validation in adaptable environments to validate system performance.

We think the intent is to allow a faster verification and validation (V&V) process so HDOs can act quickly for deployed devices. HDOs on the other side, will not assume liability of applying patches without a V&V from the MDM as it would only result in additional cost to fix if something were to go wrong and constitute potential risk to patients. MDMs that do validate and verify patches for the

customers aka HDOs take approximately 2+ patch cycles to complete their side of the testing, which in the cybersecurity standpoint is too long. This was true in case with WannaCry where it took some MDMs two or more months to even respond to the HDOs.

The whole process of patch management will be much easier for the HDO community if MDMs were to provide routine security and AV patches as part of their maintenance strategies. This will be much easier to implement despite the usual difficulty of maintaining devices that are in use, such as, patient monitors. In addition to providing timely security patches, a real incentive or consequence to do this would add to gathering support from the MDM community.

Designs that make devices easier to understand and to patch should be a mandatory requirement for any connected device regardless of its risk categorization (tier 1 or tier 2 as described in the October 2018 guidance document).

ECRI has heard of too many instances of MDMs pushing HDOs to purchase a newer platform just to fix a security problem. This issue is becoming more common as threat landscape evolves and is not always a practical and doable solution for HDOs. On the flip side there are certain platforms where we can only do so much to secure them so sometimes replacement is necessary. What is impractical is for medical device manufacturers to make cost of a necessary upgrade a barrier to a secure environment. That has elements to it that is like holding HDOs hostage. Software patch availability for both off the shelf (OTS) and vendor proprietary software should be supportable for the life of the medical device/ product as defined by the American Hospital Association (AHA) guidelines.

Delivery of these security patches would be via a third-party online portal, secure email, overnight mail, and/ or manufacturer secure portal. These are all great options, so patches can be obtained in a timely manner.

HDOs must work towards a standardized process as it relates to handling vulnerability information. At the Veterans Affairs, there is a team like one described in the MDIC publication from October 2018, that acts as a single point of communication for 140 hospitals. This team can take information from one site and send it out to the others, they collect information and deliver it to the MDMs, FDA, ECRI, and other necessary parties. The VA also communicates vulnerability information through an online portal. Accounts are set up in the portal that allows the teams to receive email updates as the national team updates the portal with security information. It would be great to see collaboration as community for a project such as this.

Because this is a regulated field – what about the FDA being the 'Responsible Disclosure' starting point)? Then the FDA tracks and discloses to the manufacturer bugs. This would provide a built-in watch-dog component if you will.

Several challenges impacting the HTM/ CE community are outlined below:

- How will the manufacturer at the time of submitting know any of this data and be able to predict future vulnerabilities. Also, it would be up to the device owner to oversee determining risk levels that are reasonable and appropriate to their situation
    - Assessment of the likelihood of a threat of a vulnerability being exploited
    - Determination of risk levels and suitable mitigation strategies
    - Assessment of residual risk a risk acceptance criterion
    - For independent service organizations this proves very difficult in trying to get patches and updates because the MDMs honestly do not care because they are not reprimanded for not providing or validating patches to known vulnerabilities
- Also mentioned is the device should be designed to anticipate the need for software patches and updates to address future cybersecurity vulnerabilities

    - More and more devices manufactures are charging for these patches through "software updates". They are basically charging for free patches that they call "updates".
- The design and architecture should facilitate the rapid deployment of patches and updates. These need to be easily accessible to the users i.e., security update section on the MDM websites.
- As for device cybersecurity end of support, especially in circumstances, like WannaCry, where Microsoft puts out a patch for legacy OS's that are not supported, MDMs should step up the game and validate patches for their devices that run on legacy OS's.

Tiered category of medical devices

ACCE believes the new tiered categorization of devices as tier 1 and tier 2 seems lacking in many aspects. It seems that tier 1 devices are devices that would be compromised in the more perfect sense, for example, hacking into a pacemaker to turn it off or remotely controlling an insulin pump to target a specific person or targeted attacks in general. The tiered system focuses largely on life/ death situations whereas large portion of cybersecurity incidents will be data related. The potential for massive amounts of compromised PHI/ PII should be a "higher cybersecurity risk" but if it poses no patient or caregiver harm (in the medical sense) then it does not fall under tier 1.

The scope in this type of categorization needs to be broadened to include unauthorized access, release of patient data, and tiered accordingly. A big goal of medical device cybersecurity is to protect patients, caregivers, and healthcare data seems to be missing from the tiered categorization.

The HTM/ CE community would also request some history behind why the FDA went with a tiered categorization (2 tiers) for cybersecurity risk.

- Tier 1 – connected and resulting in patient harm
- Tier 2 – standard cybersecurity risk, no connectivity

It would make more sense for the risk categorization to be aligned with CMS and other accreditation agency's definition of risk or to provide more clarification on how it aligns with the basic classification of medical devices as all these aspects are correlated and makes more sense as HDOs dissect to better understand and implement. There may also be added benefit in including the effect of system dependencies and other infrastructure related aspects when categorizing risk, such as, VPN, cloud, EMR integration, etc.

If a tier 2 medical device is on the same network as a tier 1 device and has open communication pathway to it, it can infect a tier 1 device causing patient harm. Additionally, even if the device does not cause direct patient harm, it can be held as ransom and cause other issues for the HDO. Therefore, we think the tiered categorization should be:

- Tier 1
    - Medical device can connect (e.g., wired, wireless) to another medical or non-medical product, or to a network, or to the Internet
- Tier 2
    - Medical device for which criteria for a tier 1 are not met

The tiered categorization of medical devices in pre-market submissions must also emphasize on disclosing system level threat models. This will be useful knowledge as it will let HDOs better understand how to manage the risk that comes with the device. Additionally, the tier 2 probability risk-based approach is poorly defined, many devices may incorrectly fall into the tier 1 category.

Password management

We think hardcoded/ default passwords are a terrible service model for MDMs to use in this age and space where threat landscape is evolving at a rapid pace. The main reason is that we have too many MDMs using default passwords is because it is easy to use and time efficient for the clinicians. In some cases, it even makes sense, such as, having 300+ bedside monitors that each have different pins to get into a 'configuration or service mode' isn't a very forgiving use model.

Some MDMs have moved to using service dongles, but this then limits the ability for in-house or third parties to be able to service the equipment as MDMs are reluctant to provide and in some cases will not even consider giving these to service dongles freely. This will then create a monopoly where MDMs are the only ones that can service the medical device.

Limiting access to a set of trusted users or maintainers can prove to be difficult for independent service organizations that service the medical device. We think the MDMs should move towards a model like what Siemens Healthcare has rolled towards, that is, HDOs and ISOs can still service the medical device without large time delays in getting correct passwords by adopting more secure ways of obtaining service passwords or keys. Mandatory passwords for basic access may not be a practical solution in every environment of care.

Documentation (MDS2, SBOM/ CBOM, risk analysis, etc.)

A lot of information that MDMs are providing right now is currently on the MDS2 and these have been made available for a while now. It is also still very hard and time consuming to gather since there is no central repository of this information. Is there a plan or process that the FDA is developing or establishing that will allow HDOs to view this information as well as download them for use?

ACCE fully supports FDA's intent to align aspects of the pre-market and post-market guidance documents with NIST CSF and documentation requirements stated in QSR 21 CFR Part 820.

ACCE's task force consists of members from the VA that have provided some essential information that is helpful for HDOs making purchasing decisions. Aspects outlined in these documents can be expanded as a general norm so there is a standard approach of evaluation across all stakeholders across the country.

- VA Directive 6550 – this document is completed by the VA and MDM before a medical device is purchased and goes onto the network. Typically, this is sent to the MDM to complete. Upon receiving the completed document, a call is setup with the MDM to review and validate/ verify additional and relevant information. This is very similar to the approach Mayo Clinic has established.
- Essential information that typically makes or breaks a purchase include:
  - A list of all TCP and UDP ports that are required for operation
  - A list of all services that are required for system operation
  - Current Operating System
  - Antivirus management
  - If the document is wireless, we require the FIPS 140-2 certification number

In addition to the above, ECRI often reviews:

- Facility security questionnaire (non-standard) – these vary in scope and depth
- MDS2

In conclusion, the American College of Clinical Engineering-ACCE believes and fully supports the FDA in that medical device cybersecurity is a shared responsibility among all stakeholders in the medical device ecosystem. ACCE is committed to participate, partner, and support approaches recommended by the FDA and will collaborate with the broader HTM/CE community to strengthen the cybersecurity practices for medical devices. Please feel free to contact me if you have any questions.

Sincerely yours,

Arif Subhan, MS, CCE, CHTM, FACCE
ACCE President
president@accenet.org
www.accenet.org

Cc: Aftin Ross, PhD (Aftin.Ross@fda.hhs.gov)