April 21, 2016

Dr. Robert M. Califf, MD
Commissioner
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Dear Commissioner Califf:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit comments on the Food and Drug Administrationôs (FDA) draft, ñPostmarket Management of Cybersecurity in Medical Devices,ò Docket No. FDAï 2015ï Dï 5105**,** published January 22, 2016.

CHIME is an executive organization serving more than 1,800 chief information officers (CIOs) and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. CHIME members are among the nationôs foremost health IT experts including cybersecurity. Within CHIME is AEHIS, an organization launched in 2014 which represents more than 500 chief information security officers and provides education and networking for senior IT security leaders in healthcare.

I. Background and Key Recommendations

CHIME and AEHIS applaud the FDA for undertaking the important topic of medical device cybersecurity. This draft guidance is intended to consider the cybersecurity issues and risks that occur after a medical device has been implemented into a healthcare delivery organization (HDO). This follows publication of FDAôs ñContent of Premarket Submissions for Management of Cybersecurity in Medical Devicesò guidance in October 2014, which was developed to help manufacturers identify cybersecurity issues when designing their products and preparing for premarket submissions. We are pleased to see the increased focus by the FDA on the critical issues surrounding cybersecurity of medical devices and their impact on patient safety. From a healthcare provider perspective, the ever increasing interconnectedness of medical devices into an HDOôs operating network has become an area of great concern. We believe an increased and formalized collaboration between the medical device manufacturers and HDOs is critical.

For several decades, there has been a tension between the identification of medical device vulnerabilities and the device manufacturerôs capability to mitigate or manage those risks. Generally speaking, when a device vulnerability is discovered or enumerated, these vulnerabilities cannot be easily rectified due to costly quality control mechanisms, such as 21 CFR Section 806. This has become even more of a problem as general operating systems, such as Microsoft Windows, are considered integral components of the medical device architecture and must be managed through these same quality control mechanisms. Security vulnerabilities resulting from these types of operating systems are occurring at a

much higher frequency than manufacturers can resolve. HDOs are generally left with managing devices on isolated and segregated networks with the hopes of reducing their exposure to threats. This, however, has proven to be ineffective. For instance, malware on portable flash drives can be easily introduced into isolated networks and then spread through vulnerable systems. Based on these concerns, we offer the following key recommendations:

1. Manufacturers should be required to configure their devices according to an industry accepted security standard that accounts for the basic principles of cybersecurity controls and alleviates risks.
2. The risk framework should be standardized and as such we encourage the adoption of a single framework across all manufacturers.
3. All risks should be reported to HDOs. Controlled risks should be reported on a regular basis (i.e. quarterly) and uncontrolled risks on an immediate basis.
4. Manufacturers should, as part of the pre-market approval process, be required to undergo a level of security validation in order to provide HDOs with a very simple and easy to implement mechanism for managing its security.
5. Use and disclosure of the Manufacturer Disclosure Statement for Medical Device Security (MDS2) should be required in all procurement transactions in order to ensure transparency between manufacturer and HDO for a proper evaluation.
6. Assuming that certain obligations can be met, postmarket guidance should incentivize the manufacturer to achieve some level of ñ*safe harbor*ò from regulatory enforcement assuming that certain obligations can met.
7. The relationship between the HDO and the medical device manufacturer should be strengthened by incentivizing participation in an Information Sharing and Analysis Organization (ISAO).
8. A core set of principles should guide the use of Information Sharing and Analysis Centers (ISACs)/ISAOs (detailed further below).
9. The definition of controlled vs. uncontrolled risks should encompass both patient safety and patient privacy issues. Cybersecurity risks in the medical device space should be classified either as ñrisks to patient safetyòor ñrisks to patient privacyòto provide a more holistic view of the cybersecurity ecosystem.
10. FDA and the Office of Civil Rights (OCR) should align their guidance and enforcement activities.
11. FDA should establish a hotline for HDOs to call should they encounter barriers with manufacturers who insist they cannot remedy an uncontrolled risk without additional FDA clearance.
12. All ISAOs should use the same format to communicate risks.

It is important to note that in many cases, it currently takes up to a decade for manufacturers to comply with new guidance or enhanced security controls. Incorporating such changes can prove extremely costly and is impacted by overall lifecycle management.

Our detailed comments are broken into three main sections: general reflections, specific commentary on the postmarket guidance, and responses to specific FDA questions.

II. General Reflections

A. Current State of Interconnected Medical Devices

The highly interconnected nature of medical devices, combined with the constraints of limited or non-existent patching cycles, has created an ecosystem ripe with technical vulnerabilities that cannot be managed in a manner similar to standard processes and procedures. The list below provides examples of a typical HDOôs challenges:

- Medical devices are being released to HDOs without basic security requirements in place such as: encryption, access control mechanisms (the ability to positively authenticate to the device), hardcoded default passwords which cannot be changed, and excessive administrative database rights granted by service accounts without the ability to restrict access.

- Vulnerabilities discovered within medical devices cannot be patched or mitigated in a timely manner due to the requirement that device manufacturers follow extensive quality control processes. Additionally, in many cases it is not possible to patch a device without first investing in an upgrade to newer versions. Upgrades can be quite costly and usually require long planning cycles in order to secure the correct budget. Purchasing new equipment to remediate security vulnerabilities is not always the best or most realistic answer for the healthcare industry.
- Medical devices are increasing their storage capacities, which potentially increases the amount of protected health information (PHI) stored on these devices. This creates significant risk to patient privacy and compliance challenges with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).
- There are no expiration dates on FDA pre-marketing clearances for medical IT devices despite medical device manufacturer and FDA knowledge of end of support dates for major operating systems.

The Office of the National Coordinator (ONC) oversees certification programs that govern the function, security, reporting and interoperability of electronic health records (EHR). However, the Department of Health & Human Services (HHS) does not have similar regulatory oversight for medical devices with inherent risks to patient safety, care effectiveness, or data security. **We recommend HHS introduce a certification program for the medical device industry to ensure that devices being purchased have met vigorous testing and cybersecurity quality controls.**

B. Patient Safety vs. Privacy of Patient Information

The FDA postmarket guidance specifically addresses patient safety related cybersecurity risks. This is critically important, especially considering the alert that was issued in May 2015 on a vulnerability identified with an infusion system. However, this guidance does not directly address risks to patient privacy. Although some patient privacy risks will be addressed in concert with the patient safety issues, it is quite possible that a risk to patient privacy might not be evaluated as an ñuncontrolledò risk, and therefore will not be resolved in as timely a manner as the HDO would expect.

As evidenced by Executive Order 13636, dated February 12, 2013, ñImproving Critical Infrastructure Cybersecurity,ò as well as, the recently passed Cybersecurity Act of 2015 (part of the Consolidated Appropriations Act of 2016), cybersecurity has become a greater national priority. Section 405 of the Cybersecurity Act of 2015 specifically calls on HHS to deliver a plan to Congress within one year detailing how it will address cybersecurity issues in the industry. Further, the HHS cybersecurity taskforce formed by this law is directed to advise the secretary on the ñchallenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record.ò **We recommend that the FDA and OCR work together to better align and coordinate their implementation guidance in order to provide a holistic cybersecurity ecosystem.**

Manufacturers should be required to configure their devices with respect to an industry-accepted security standard; a standard that accounts for the basic principles of cybersecurity controls and alleviates these risks. Other industries have introduced similar validation schemes, such as the PA-DSS validation within the PCI-DSS (both involving the payment card industry). Also, EHR vendors must meet certain standards in order to be certified by ONC. Device manufacturers should go through a similar level of certification, allowing HDOs to easily understand and implement security protocols. Additionally, **the use and disclosure of the MDS2 should be required in all procurement transactions.**

Further, the postmarket guidance should grant manufacturers with some level of "safe harbor" protection against regulatory enforcement, provided that they achieve third-party certification, actively participate in a centralized ISAO and develop security patches in a timely manner. Minimum requirements for these obligations would be: 1) transparency with the HDOs of risks identified within their devices in a reasonable time period; 2) participation and collaboration of the manufacturers with HDOs to resolve discovered vulnerabilities; and 3) nimbleness in responding to reported vulnerabilities whereby manufacturers will proactively work with HDOs to mitigate known vulnerabilities in a timely fashion.

We note, however, that not all HDOs can afford to participate in one or more ISAOs. Therefore, we highly recommend that the creation of ISAOs be limited in order to reduce the likelihood of an overly complex system. Additionally, the verification process needs to take place during the premarket approval process, and therefore should be added to the premarket guidance document. We will provide further commentary on these requirements as part of our comments on ñuncontrolled risk.ò

Even if manufacturers enabled all of the basic security controls noted above, it would take upwards of 10 years for HDOs to reap the benefits of these new practices. This is due to the long life cycle of many medical devices, especially the more expensive systems such as MRIs. As such, there needs to be a transitory path the industry can follow for the next decade until such a level of maturity can be achieved.

III. Specific Commentary to the Postmarket Guidance

CHIME and AEHIS have addressed the postmarket guidance document based on five sections:

A. Information Sharing and Analysis Organizations
B. Definitions of ñControlled Risksò vs ñUncontrolled Risksò, and the challenges this might introduce
C. Medical Device Risk Analysis and Risk Management
D. Specific feedback on management of ñControlled Risksò
E. Specific feedback on management of ñUncontrolled Risksò

A. Information Sharing and Analysis Organizations (ISAOs)

The majority of CHIME and AEHIS members have been or are currently members of an ISAC. Some examples include the National Healthcare ISAC (NH-ISAC), or the Research and Education Networking ISAC (REN-ISAC). The benefits of ISAOs/ISACs include the ability to:

- Share cyber threat and vulnerability information with clearly defined protections of confidentiality amongst the participating organizations.
- Share cybersecurity challenges in an ad-hoc manner amongst peer institutions thus assisting the industry in raising its cybersecurity maturity levels.
- Consume threat intelligence information in an automated and real-time manner with the assistance of third-party ówatchdogôgroups to provide additional context to already strained internal information security teams.

Current ISAO/ISAC participation involves HDOs and only a handful of third parties. The **relationship between the HDO and the medical device manufacturer should be strengthened through incentivizing participation in ISAOs. As stated earlier, we feel this participation should be a requirement for enabling any safe harbor activities that might be granted. That said, we also believe that the effective use of ISAOs/ISACs can only be achieved through manageable relationships. The following principles should be considered as guidelines:**

- The number of ISAOs/ISACs should be limited; an ISAO should not be created out of any particular groupôs need. For example, the creation manufacturer-specific ISAOs would be duplicative, costly and ultimately not actionable.
- The costs of ISAOs/ISACs must be controlled, especially if the formation of the ISAOs will be unmanaged. Many HDOs have tight budgets and costs should not be a barrier to entry for the protection of this critical infrastructure. Further, manufacturers should help share the burden of these costs in order to increase HDO participation.
- **The sharing of actionable cyber threat information must leverage a common format among all ISAOs/ISACs.** This is a critically important principle since the information that is generated from the ISAOs must be actionable by the receiving HDO. We encourage adopting open standards, such as those supported by the OASIS project, and more specifically the Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) and Cyber Observable eXpression (CybOX) framework for sharing this information.

- Encourage all ISAOs to participate in the United States Computer Emergency Readiness Team (US-CERT). In this manner, relevant and actionable information can be provided to those HDOs that do not currently participate in an ISAO.
- The disclosure and notification of vulnerabilities should be provided directly to the HDO, as well as through the US-CERT. We are not opposed to leveraging the ISAOs as a means for disclosing vulnerability data, especially as it relates to the evaluation of risk, however, we believe that the ISAOs should be at the core of a collaborative group for sending and sharing sensitive materials. Ultimately, the disclosure of vulnerabilities is something to be consumed by the public for executing appropriate risk mitigation processes.
- Consideration needs to be given to how best ensure disclosures of confidential information shared by providers within an ISAO are done in a manner that does not jeopardize reputational harm (i.e. use of non-disclosure agreements). There should be mechanisms supported by the appropriate federal agency that protect organizations participating in the ISAOs from accidental releases of confidential information.

B. Definitions on "Controlled Risks" vs "Uncontrolled Risks"

FDA has divided risk into two classifications: controlled and uncontrolled, with a focus on patient safety. Ultimately, the level of risk is based on whether or not a vulnerability impacts the "essential clinical performance" of the medical device. Those that do impact its performance will be categorized as "uncontrolled risks" and require certain actions to take place. "Controlled risk," FDA states, "is present when there is sufficiently low (acceptable) residual risk that the device's essential clinical performance could be compromised by the vulnerability." On the other hand, the agency states that "uncontrolled risk is present when there is unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient risk mitigations and compensating controls. If the risk to essential clinical performance is assessed as uncontrolled, additional risk control measures should be applied." FDA goes onto note that "manufacturers should define, as part of risk management, the essential clinical performance of their device, the resulting severity outcomes if compromised, and the risk acceptance criteria." We appreciate the simplification that the two risk models of "controlled risks" and "uncontrolled risks" provide. Nonetheless, we would like to offer some suggestions around further defining the risk model.

First, we are concerned that unless these terms are further clarified, a manufacturer may perceive controlled vulnerabilities as acceptable and thus require no further action. We are particularly worried that those risks that are not related to patient safety, such as privacy, could be ignored unless guidance is clarified. Second, we believe that the terms as outlined could pose confusion for some. For instance, when you use the term "controlled risk," a person who is not experienced in security issues could easily conclude that no action is required and that everything is "ok." It is important that personnel who are not information security experts understand these terms. And third, FDA has indicated it might not enforce further action on "uncontrolled risks" by manufacturers when there is: 1) no known serious adverse event; 2) within 30 days of learning of the vulnerability the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users; and 3) the manufacturer is a participating member of an ISAO, such as ISAC. FDA has still called for manufacturers to report these risks to their customers. We firmly agree that all risks should be communicated to HDOs (see our response to Q2 concerning communication). We continue to have concerns that even though the FDA has called for manufacturers to provide HDOs with temporary measures to mitigate the risk, the recommendations - as we have seen in previous guidance - can cause significant operational harm to the HDO. For instance, when vulnerable medical devices are disconnected from the wireless network and operate in "standalone mode" this shuts down all integrations and interconnectivity between these devices and downstream systems that require manual processes to take effect; this causes significant operational overhead on the HDO and can create patient safety and interoperability issues.

Given these concerns, we recommend that FDA issue two sub-categories under both "controlled" and "uncontrolled" risks. The first sub-category would be aimed at patient safety and the second aimed at information risks (in particular, though not limited to, privacy issues). FDA should work collaboratively

with OCR to share information risks that are related to patient privacy. This would be consistent with what is called for in the earlier referenced Executive Order and Cybersecurity Act.

We also believe that inserting the word ñpatientò into each category would make the labels more meaningful. We have outlined our ideas for a revised risk model categorization below:

1. **Controlled Patient Risk**
    a. **Patient Safety Risks**
    b. **Patient Information Risks**
2. **Uncontrolled Patient Risk**
    a. **Patient Safety Risks**
    b. **Patient Information Risks**

Under our schema, Patient Safety Risks would involve data stored on a device or transmitted to or from the device. Included in this would be issues associated with data integrity. We have concerns that an attack on a medical device to alter the data collected (resulting in a risk to the integrity of the device and its data) could have severe downstream patient safety impacts. If the data were corrupted it could result in clinicians making decisions based on faulty information that could result in patient safety issues. As an example, a blood pressure monitor could raise systolic measurements consistently by 40-50 where a patient is actually at normal or low blood pressure causing the clinician to order a medication to be administered and the patient to have a blood pressure crash.

Patient Information Risks on the other hand would focus on issues that are not safety-related but could cause other harms to patients such as loss of privacy, a vulnerable device being used as a pivot for further attack into the HDOs network, or issues stemming from power failure. **We firmly believe that issues around patient privacy are paramount and warrant a separate category and risk calculation.** In subsections C and D below we have outlined how the parameters of our schema could work.

C. Specific feedback on management of "Controlled Risks"

As noted above, we believe the definitions of ñcontrolled riskò need to be broken down into patient safety risks and patient information risks. Below are our ideas for how this could be structured.

Controlled Patient Safety Risks

- The risk does not have a direct or indirect impact against the clinical effectiveness of the medical device. In other words, there is no direct impact to patient safety due to the risk existing.
- There should be a cycle where the manufacturers are disclosing this information to HDOs. This should not necessarily have to go through the ISAO but rather through other communication channels including directly to known customers and via the US-CERT (see our response to Q2 concerning communication).

Controlled Patient Information Risk

- Privacy risks would be encapsulated under this category, as should other items that may not be patient safety risks (i.e. pivot attacks and power failure related risks).
- HDOs need to know about these types of risks since the implication of the risk could have different impacts during implementation of the device. For instance, a HDO could implement the device with a vulnerability that permits an attacker access to the HDO network, however causes no uncontrolled risk to patient safety. From the HDO perspective, this vulnerability would be leveraged for further attack against the HDO and, as such, the HDO would want to enumerate and mitigate the risk in an appropriate manner (including partnering with the manufacturer and removing the vulnerability).

D. Specific feedback on management of "Uncontrolled Risks"

Generally speaking, our members believe that more scrutiny of manufacturers is needed when patient safety risks are identified.

Uncontrolled Patient Safety Risks

- If the manufacturer is reporting in good faith we agree that the guidance, as outlined, seems appropriate. However, we continue to worry about exhaustive quality assurance (QA) processes that manufacturers report they must follow when a risk is identified and using those QA processes as reasons why the inherent vulnerabilities cannot be mitigated. **To that end, we recommend the FDA establish a hotline for HDOs to call should they encounter barriers with manufacturers who insist they cannot remedy an uncontrolled risk without additional FDA clearance.**
- **If an Uncontrolled Patient Safety Risk is identified then we feel this risk should be monitored by a third party over the manufacturer in order to ensure the risk is effectively mitigated (i.e. similar to the way PCI works.)**
- Further detail regarding the specifics of uncontrolled risks needs to be better identified. For instance, an alert noting an issue with an infusion pumpôs ability to administer a drug may read, ñMalfunction of delivery mechanismò which is not enough. An HDO needs to know whether the issues stems from the operation system, hardware, software, the network, or something else. HDOs need sufficiently detailed information so they can enact their own risk management techniques. Microsoftôs vulnerability disclosures have a prescribed format that is consistently used and could be looked to as a starting point.
- All ISAOs should use the same format to communicate risks. We believe NIST could be a good partner to help develop this.
- For recalls of equipment that involve Uncontrolled Patient Safety Risks but are outside of the warranty, manufacturers should still be required to report these issues so the HDO can be enabled.

Uncontrolled Information Risks

- The risks described within this category are those that would directly relate to the confidentiality of the patientôs information stored on, or transmitted from, the devices.
- Risks within this section would be items that could lead to the eminent disclosure of patient information in an unauthorized manner, thus creating the potential for a HITECH-related breach event.

E. Medical Device Risk Analysis and Risk Management

Manufacturers will be required to manage risk throughout the deviceôs lifecycle, which includes: 1) assessing exploitability of vulnerabilities (and the introduction of a new type of Common Vulnerability Scoring System (CVSS) scoring mechanism); 2) assessing the impact to a patientôs health (scoring on a 5 part impact scale); and 3) leveraging these two factors to determine the resulting risk of the clinical effectiveness, falling within either ñcontrolledò or ñuncontrolledò risk.

If manufacturers are permitted to assess their risks, evaluate the results of those vulnerabilities/impacts, and be granted a safe harbor by participating in an ISAO, they could be incentivized to place themselves in a controlled risk state rather than an uncontrolled risk state. We believe in the principle of providing manufacturers safe harbor if they disclose, but there should be checks-and-balances from the assignment of controlled risks themselves. This is the area where we feel third-party oversight could help assist the process. We also encourage the disclosure of all identified controlled risks to HDOs on a periodic cycle (perhaps quarterly) with the agreement to take feedback from the HDOs on their risk calculation and adjust as necessary, if sufficient. This will provides a feedback mechanism from the HDOs into the risk management process itself. If there are additional abilities to implement additional controls to manage the controlled risk HDOs should know about that sooner so they can take actions.

We also believe the risk framework should be standardized, not just offered as guidance. This is very important in order to provide consistent application of the difference between ñcontrolledò and ñuncontrolledò risks. If manufacturers introduce their own risk models the practice of ñcontrolledò and ñuncontrolledò risks will vary dramatically. This will cause undue burden on the HDO for executing its own risk management techniques. As such, we encourage the adoption of a single framework across all manufacturers.

We are supportive of leveraging CVSS scoring for the identification and enumeration of vulnerabilities. We are not convinced that a new factor should be added to the CVSS scoring mechanism strictly for medical devices or patient safety, given that the CVSS scoring system is universal, multi-industry and abstract. We feel the evaluation of the vulnerabilities through the CVSS scores, however, would be a very important factor in the overall risk calculation.

Regarding Patient Information Risks, the current model only addresses patient safety. Impact statements will need to be adjusted if privacy considerations are going to be taken into account. A potential scale for determining the impact of Uncontrolled Information Risks could be:

- *Negligible*: Access of any non-patient related information (nothing individually identifiable, or protected health information).
- *Minor*: Would need to have access to multiple systems to recreate identifiers and the actual original PHI.
- *Serious*: Ability to exploit a medical device, either electronically or physically, and gain access to electronic PHI (ePHI) in an unauthorized manner.
- *Catastrophic*: Ability to modify data that could cause patient harm (through device itself or changing information that goes back to the EHR that provides inaccurate clinical decision support).

IV. Answers to FDA specific questions on ISAOs

Q1. What factors contribute to a manufacturer's decision whether or not to participate in an ISAO?

We defer to the manufacturers.

Q2. ***In the draft guidance, the FDA is proposing its intention to not enforce certain regulatory requirements for manufacturer's that are ''participating members '' of an ISAO. Should FDA define what it means to be a ''participating member'' of an ISAO and if so, how should such participation be verified?***

At a minimum, participation attributes should include membership in an ISAO. Other key attributes should include submitting information into the ISAO for digestion or reacting to information from others. These responses should be timely and objective and detailed. When manufacturers determine vulnerabilities exist they should be required to:

- Provide information to all HDOs regardless of ISAO participation;
- Push the information out via US-CERT; and
- Communicate the information directly to their client base since HDOs might act on targeted information like this especially if it is highly critical and where there are patient concerns. An example of this would be a virus is detected on a pacemaker. The manufacturer should not only be required to post information on their website but to also actively push for getting the firmware updated to resolve the issue.

We also believe that in order to help HDOs manage the financial burden of participating in ISAOs that manufacturers could be incentivized to assist with this financial obligation as part of the classification of ϕparticipationô

Q3. What are the characteristics (participation, expertise, policies, and practices) of an ISAO that would make it qualified to participate in the sharing and analysis of medical device cybersecurity vulnerabilities?

Please see our response detailed under Section III. In addition, we strongly suggest that the ISAO not be used as the only a mechanism for notification. Rather should be a vehicle by which HDOs, manufacturers, and security researchers can discuss, uncover risks, and validate their solutions. This provides two benefits:

1) Hospitals with limited resources aren't left out of communication about risks and resolutions; and 2) ISACs are not cluttered-up with members who can't participate meaningfully and/or appropriately.

Q4. What are the benefits and disadvantages of FDA 'recognizing' specific ISAOs as possessing specialized expertise relevant to sharing and analysis of medical device vulnerabilities and what should such recognition entail?

CHIME and AEHIS strongly recommend limiting the number of ISAOs. We recommend that there be only one, or at the very least, only a few within this sector since we believe that multiple ISAOs will only bring complexity. The proliferation of ISAOs could become overly burdensome. Also, as noted earlier, we recommend there be a single method, methodology and taxonomy for communication (such as STIX and TAXII).

Q5. When cybersecurity vulnerability information is not reported to FDA, what information should be reported to the ISAO, and when?

We recommend that all risks be reported to the HDOs. As noted earlier, controlled risks could be reported on a quarterly basis and uncontrolled risks on an immediate basis. Additionally, we feel the ISAOs can assist in the following manner as part of this reporting process:

- Engaged discussion and assistance in the evaluation of the disclosed risks.
- To be a safe place for manufacturers, HDOs, security researchers, and the government to uncover, discuss, research, validate risks and their solutions.
- To be a safe place, everyone must be able to feel comfortable that information they place in the ISAO can't be used against them. Competing manufacturers should not be permitted to use the information discussed within an ISAO for a competitive advantage.
- To be a safe place for HDOs to post sensitive information (such as log files) for assisting in security research without the fear of a competing institution using that for a competitive advantage (such as conducting negative ad campaigns on a neighboring hospital system).

Q6. How should the FDA interact with ISAOs, manufacturers, HDOs, security researchers and other stakeholders to maximize the sharing of information concerning cybersecurity threats while maintaining confidentiality and protecting commercial confidential information?

From an HDO perspective, we believe that providers want to contribute what they know but also be held harmless for their contributions. There is a level of uncertainty among many HDOs around what is needed from a HIPAA perspective in terms of sharing information. ISAOs are membership organizations that are not overseeing PHI. For an ISAO to protect PHI then they need to obligate all members to protect it. Any time privacy vulnerabilities are identified there should be collaboration with the manufacturer. Everyone who signs up for the ISAOs should be assuming the obligations of protections for all memberships. To join, we believe you need to take on the responsibility of managing the confidentiality. Unfortunately, this is another reason why not everyone will sign up for them.

Examples of the types of questions that have arisen around HDO relationships with ISAOs that warrant clarification from OCR include:

- Is an HDO required to have a BAA with an ISAO when sharing threat information (even if they are not purposefully sharing PHI)? If there is no BAA in place and PHI accidentally gets shared would this be considered a breach?
- Does the definition of health care "operations" account for information shared with an ISAO?
- Would an HDO provider need to have a BAA in order to take advantage of any flexibility offered under "operations" (assuming such existed) or could they still take advantage of this without one?

In conclusion, we feel there needs to be a process and responsibility imposed upon its participants to protect patient information and maintain confidentiality. HDOs want to contribute what they know and be held harmless for their contributions.

V. Conclusion

CHIME and AEHIS appreciate the opportunity to offer our collective perspective. We stand ready to working collaboratively with the FDA and other agencies to reduce cybersecurity risks. Should you have any questions about our comments please direct them to Mari Savickis, vice president, federal affairs at msavickis@chimecentral.org.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Marc Probst, CHCIO
Chair, CHIME Board of Trustees
CIO, Intermountain Healthcare

Deborah Stevens
Chair, AEHIS Board of Trustees
CSO, Tufts Health Plan