April 28, 2016

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Information Management Executives (CHIME) is pleased to submit comments on the Food and Drug Administrationôs (FDA) draft guidance, ñDesign Considerations and Premarket Submission Recommendations for Interoperable Medical Devices,ò Docket No. FDA-2015-D-4852, published January 26, 2016.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.

General Comments

Hospitals and physicians have invested billions of dollars adopting electronic health records (EHRs), purchasing devices, installing interfaces, and pursuing an interconnected ecosystem. They have made significant strides over the past decade in digitizing health care with an eye towards improving quality and increasing efficiency. However, significant barriers remain to creating a truly interoperable system. Our members strongly support FDAôs efforts to improve device interoperability, especially given the proliferation of devices used across the health care system.

Nonetheless, CHIME members are concerned that the draft guidance represents a set of suggested principles. CHIME members seek assurance that the devices they purchase are able to connect with other devices and systems. For instance, our members struggle with ensuring that the devices they purchase and the data that is generated (to the degree that a device is even able to do this) will connect with their EHR systems and that they provide clinicians with the real time information they need to deliver patient care. When purchasing devices many providers are told that the devices are ñinteroperable.òHowever, once purchased, providers learn that in many instances they need third party software to connect the device to the EHR. This adds unanticipated costs and complexity to the health care system and is a barrier to providing clinicians with the information they need at the point of care. Additionally, our members also report a lack of transparency around the standards used by manufacturers impacts interoperability and data flow. Finally, we also believe that transparency is necessary in order to achieve a more secure healthcare ecosystem. This is discussed in our comments to FDA on their draft Postmarket guidance on device cybersecurity.

CHIMEôs top recommendations are summarized below. **Specifically we recommend FDA:**

1. **Collaborate with the Office of the National Coordinator (ONC), providers, device manufacturers, other appropriate stakeholders to establish a baseline set of uniform interoperability standards for devices that must be met in order to receive FDA approval.**
2. **Work with ONC and interested stakeholders to establish a more robust definition of interoperability.**
3. **Work with ONC to have them certify APIs.**
4. **Synchronize efforts across with other federal agencies in applying risk management principles.**
5. **Require that device manufacturers to perform a risk assessment annually on their devices.**
6. **Ensure alignment between the FDA's cybersecurity guidance for device manufacturers and the interoperability guidance.**
7. **Require device functionality receive the same level of transparency as EHRs.**
8. **Create a central, online database that includes key functionality of devices (i.e. interoperability and security).**

Specific Comments

I. Introduction

FDA acknowledges that the tremendous growth in the use of medical devices hastens the importance of creating an interconnected ecosystem and effective exchange of patient data. However, the agency also points out that its guidance document does, ñnot establish legally enforceable responsibilities.òYet, FDA also notes that, ñAs electronic medical devices are increasingly connected to each other and to other technology, the ability of these connected systems to safely and effectively exchange and use the information that has been exchanged becomes increasingly important.ò

CHIME is in full agreement that there has been a proliferation in the number of devices which are increasingly connected to one another and that considerations around patient safety are paramount. That is precisely why we believe FDAôs guidance should require device manufacturers be transparent about device functionality. In many cases, interoperability issues exist which are outside of a providerõs control. The advent of new technologies and a growing ñinternet of thingsò creates an environment where interoperability is expected. In the absence of such transparency, providers struggle to address issues that affect patient safety and protecting patient information. Adding to these concerns, manufacturers shield themselves from taking what providers believe are needed actions to better secure and ensure devices interoperability.

II. Background

Need for Greater Transparency

CHIME agrees with FDAõs position that ñinteroperability in healthcare has the potential to encourage innovation and facilitate new models of health care delivery by promoting the availability and sharing of information across systems even when products from different manufacturers are used.ò We do not believe, however, that the desired end state of interoperability will be achieved unless more emphasis can be placed on requiring manufacturers be more transparent about device functionality. Further, we believe there is an intersection between interoperability and cybersecurity and that increased and formalized collaboration between medical device manufacturers and providers, as it relates to cybersecurity, is critical. We have submitted separate comments to this end on the FDAõs draft Post-Market guidance on cybersecurity of medical devices.

FDA also notes in the background section that, ñDesign elements that factor into interoperability considerations may improve data portability and patient safety. However, errors stemming from inadequate interoperability can occur, such as the transmission of weight in kilograms when the receiving medical device assumes the measurement is in pounds, and can lead to patient harm and even death.ò Our members strongly agree with this sentiment. Our members report pediatric devices are particularly affected by these issues. They believe that because the market for pediatric devices is not as large as the one for adults, that there is less competition and less incentive to innovate. In some cases (e.g. hearing test devices for infants), only two vendors compete, and each one implements its own data format and transmission protocol. These devices have not been engineered to send data to EHRs, so providers must purchase an intermediary device to achieve interoperability. In situations such as these, providers must take the data from devices and convert elements such as weight manually before including it into the medical record.

Some manufacturers have told CHIME members they donõt use a uniform set of standards because, ñThey are not required to.ò Data formats and transmission protocols vary across devices, pediatric or for adults; yet providers need a uniform set of standard. Having this would go a long way to furthering interoperability. **CHIME strongly recommends that the FDA work collaboratively with ONC, providers, device manufacturers, and other appropriate stakeholders to establish greater transparency around standards used by device manufacturers.**

Definition of Interoperability

On lines 144-146, FDA refers to interoperability as, ñThe ability of two or more products, technologies or systems to exchange information and to use the information that has been exchanged.ò Later on line 235 the guidance states, ñFor purposes of this guidance, interoperable medical devices are devices as defined in Section 201(h) of the Federal Food, Drug, and Cosmetic Act that have the ability to exchange and use information through an electronic data interface with another medical device, product, technology, or system. Interoperable medical devices can be involved in simple unidirectional transmission of data to another device or product or in more complex interactions, such as exerting command and control over one or more medical devices."

We have a number of concerns with these definitions. First, we believe they are insufficient. We firmly believe there is a need for standardized and structured exchange of information that allows for the harmonization of data sets between medical devices, medical applications, and healthcare provider systems. Today, providers must use certified EHRs in order to avoid a financial penalty under the Medicare Meaningful Use program and under a growing number of other Medicare programs. EHRs must meet certain standards in order to be certified. While challenges still exist connecting disparate EHRs, the use of a baseline set of standards is the first step on the path towards achieving interoperability. Unfortunately, unless device manufacturers use agreed upon standards, the interoperability problems we see today are only going to grow as more devices are added to the system.

Second, although the term interoperability is often used, there has been no widely agreed upon definition within HHS. ONC recently published a RFI on this very topic. **We recommend that the FDA work with ONC and interested stakeholders to establish a more robust definition of interoperability.**

Third, our members have encountered numerous instances in which there is a gap between vendorsôand providersôdefinition of interoperability. While claiming interoperability, vendors implement proprietary interfaces and data communication protocols. This situation is often revealed, unfortunately, after the purchase has been made and the devices were delivered. In many cases, in order to connect devices to EHRs and other systems, providers need to purchase additional middleware which is cost prohibitive. The middleware is needed to extract data from devices, convert and format data in a uniform manner, and communicate with EHRs. The inclusion of the middleware increases the complexity of the system, reduces its reliability, introduces additional security risks, and increases the overall cost of the system.

There is also no recourse for a provider if they experience challenges with device interoperability. While members report that manufacturers are generally more responsive to critical issues with devices that has not been the case with interoperability. One member commented that device interoperability challenges are a, ñblack hole when you report to the manufacturer and FDA.òThere is, however, a strong nexus between patient safety and interoperability, which is something we urge the FDA to recognize.

Finally, the challenges with device interoperability could also be perceived as ñdata blocking.ò Data blocking has been deemed unacceptable by the secretary, and CMS and ONC have this issue squarely in their cross hairs. CMS administrator Andy Slavitt has been quoted as saying on numerous occasions that he is, ñdeadly serious about interoperability.ò The need to constantly purchase middleware is a drain on the health care system and is unsustainable. As provider reimbursement evolves to a system that is increasingly focused on outcomes, the ability to move data seamlessly will drive better care coordination and ultimately better patient outcomes. If providers are forced to continue to invest in middleware to move data, then these costs will come at the expense of other patient care investments.

CHIME strongly urges the FDA to work collaboratively with ONC, CMS, providers, device manufacturers, and other interested stakeholders to establish a baseline set of uniform interoperability standards for devices.

National Patient Identification

On lines 182-184 FDA states, ñSpecific information, such as UDI (unique device identifier), and patient-specific data, such as ECG waveforms, contained within a medical device can contribute importantly to patient care and improved patient outcomes.ò We support the adoption of a UDI standard. With regards to patient identification, CHIME feel strongly this is a critical issue and is a leading advocate for a solution that uniquely and accurately identifies a patient 100 percent of the time. From a patient safety perspective, we believe having both solutions is far preferable to using the UDI alone. CHIME is partnering with HeroX prize on a $1 million competition to incent innovators to develop a solution a one million dollars to the winner of this contest seeking a solution. A winner is expected to be announced in or around February 2017.

III. Scope

No comment.

IV. Definitions

A. Electronic Data Interface

On lines 229-233 FDA states, ñFor purposes of this guidance, electronic data interface (EDI) is the medium by which independent systems interact and/or communicate with each other thereby allowing the exchange of information between systems. It includes both the physical connection (i.e. USB port, wireless connection, etc.) and the data schema which defines the information content. It is a medium by which a medical device exchanges and uses information.ò EDI must also contain API functionality and specifications. The industry is already at the point where APIôs are being developed to interconnect a medical device to an app. Therefore, EDI is not just a wired or wireless connection; itôs also an API or as one of our members explains it, ña suspension bridge to connect the highways together.ò

B. Interoperable medical devices

Please see our above comments under Section II.

V. <u>Design Considerations for Interoperable Devices</u>

As noted earlier in our comments, we believe it is in the best interest of providers and patients if FDA coordinates closely with ONC to help ensure the intended outcome of device interoperability is achieved.

Also, on lines 256-259 FDA says, ñManufacturers of interoperable medical devices should perform a risk analysis and conduct appropriate testing that considers the risks associated with interoperability, reasonably foreseeable misuse, and reasonably foreseeable combinations of events that can result in a hazardous situation.ò Our members recommend FDA catalogue the risk analysis findings, which would prove useful during a providerôs procurement process. This could be part of a centralized place that details information about the devices, as discussed elsewhere in this letter.

A. Purpose of the Electronic Data Interface

On lines 309-339 FDA lists the elements a manufacturer should consider in the design of the deviceôs electronic data interface. The last item listed is, ñExpected flow of information or exchange of information through an application programming interface (API) which may include considerations of acceptable and unacceptable commands on the interface and impact of such interface on the device safety and effectiveness.ò We agree with this. Clear, comprehensive documentation of the API functionality, together with the uniform set of standards (mentioned previously) are essential for true interoperability. **Specifically, we recommend FDA work with ONC to have them certify APIs.**

We would also note that the ñPatient Electronic Access to Health Informationò objective of the Stage 3 of the Meaningful Use program already requires that vendors incorporate ONC-certified APIs into their EHRs and providers enable these to provide patients with an additional method to ñView, Download, Transmitò their records. As written, the objective provides for read-only APIs to allow the patients to download their information. In the case of medical devices, however, bidirectional interfaces and APIs that facilitate two way exchange of information are very important in order to reduce the need for manual data entry. For example, devices should be able to receive Admission-Discharge-Transfer (ADT) messages to automatically create patients worklists without error-prone human intervention

B. Anticipated users

FDA calls on manufacturers to, ñIdentify not just the purpose of the electronic interface, but also the anticipated users of the electronic data interface.ò In order to increase the security of the device (and indeed of the system), we recommend that device manufactures implement access control capabilities and that the use of generic user accounts on connected devices be discouraged. Authentication and authorization functionality should be strongly recommended. Consideration should be given to devices being able to use open authentication and authorization standards such as LDAP and OAuth Version 2.0.

C. Security and Risk Management Considerations

Under risk management, FDA calls on manufacturers to, ñConsider ways to mitigate all risks identified in risk analysis, such as risks that arise from others connecting to the electronic data interface including the risk of inappropriate access to the device.ò We support the sentiment, however, as noted above, more transparency is necessary in order to achieve a more secure healthcare ecosystem.

Our members continue to assert that if they are going to be held responsible for being in compliance with OCR requirements (i.e. HIPAA and HITECH) and for performing periodic risk assessments, they need clear rules detailing what is and is not acceptable from a compliance standpoint. **CHIME recommends more alignment within the federal government in applying risk management principles.** This is important for our nationôs healthcare providers on whom the burden of protecting patientsô PHI falls squarely as HIPAA covered entities.

Additionally, providers are required under HIPAA, and as part of meeting the Meaningful Use requirements, to conduct a risk analysis. Providers are required to do this annually to meet Meaningful Use. On the other hand, device manufacturers are under no obligation to perform these risks assessments, which are only ñsuggestedò activities. Itôs hard to imagine how providers can perform thorough, meaningful risk analyses when critical components of the infrastructure (i.e. connected medical devices) are left out. **We urge the FDA to require device manufacturers perform a risk assessment annually on their devices.**

We also want to raise concerns around the need for device encryption. On lines 267-269 FDA states, ñAs part of a comprehensive quality system under 21 CFR Part 820, medical device manufacturers must manage risks including those associated with an electronic data interface that is incorporated into the medical device.ò We strongly agree that risks must be better managed. As part of this section, we urge FDA to consider the need for encryption, including transmission of data. Our members continue to report that medical devices are being released to providers 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.

Importantly, we also want to emphasize that even if information is being shared in a standardized manner, it also needs to be authenticated. To that end, we are concerned with the lack of access control, including authentication requirements for devices, which has led to a situation described by one member as the ñwild, wild west.ò Without access control there are some devices where anyone can walk into a room and change the device. We want to move away from the environment we have today where manufacturer-set passwords are commonly used which cannot be changed by the provider creating security and interoperability risks. **We recommend FDA: 1) require device manufacturers be more transparent around how they handle authentication; 2) consider more emphasis be placed on use of digital certificates and that open standards for authentication and authorization such as LDAP and OAuth Version 2.0 be encouraged; and 3) tightly aligned interoperability guidance with FDA cybersecurity guidance.**

D. Verification and Validation Considerations

Under this subsection FDA says, ñIf the medical device is meant to be a part of a larger interoperable system, the manufacturer should conduct testing to reasonably assure that the medical device will continue to safely and effectively fulfill its intended use when it is assembled, installed, and maintained according to its instructions.ò We agree.

FDA notes that, ñA manufacturer should design an interoperable device that can mitigate risksò and lists a number of specific scenarios including, ñFailures or malfunctions caused by invalid commandsò on line 413. We are unclear how manufacturers will define an invalid command. We recommend ñinvalid commandsò be clarified under the definitions section and that the FDA provide a uniform set of requirements or standards to help define.

E. Labeling considerations

FDA calls on manufacturers to, ñInclude information that users may need to connect predictably and safely to the interface for its intended purpose.ò Our members found the concept, as outlined in the guidance document, confusing. The term ñlabelingò did not resonate with them as they donôt envision a device coming in a box with a label. Performance information should be clearly conveyed on manufacturersô websites and, ideally, in a central repository housed by Health & Human Services (HHS). For example, one member reported significant challenges trying to get their vital signs devices interconnected. This has required a substantial amount of back and forth with the vendor. **We recommend renaming this section to be called, “Transparency of Device Performance.”**

EHR vendors are required by ONC to report certain details about their products that are listed on the ONC website known as the Certified Health IT Product List or CHPL. The secretary, the CMS administrator, and the national coordinator for health IT have called for the need for greater transparency in the marketplace. ONCôs final rule on Version 2015 of EHR certified software includes even greater requirements for vendors on transparency for their products. **We believe the same level of transparency is needed for devices and urge the FDA to create a central, online database that includes key functionality of devices (i.e. interoperability and security).** Doing so will increase the ability for providers to be better informed consumers and will put pressure on the vendors to be forthcoming with the functionality of their products. As mentioned previously, vendors and providers often have different definitions of what interoperability is and how it is accomplished. The ability to electronically transmit and use the data from medical devices is not a ñnice to haveòfeature anymore, but a critical aspect of healthcare. EHRs are only one piece of the health care ecosystem and treating devices differently will not allow the nation to achieve the desired interoperability.

Last, our members experience tremendous problems with extracting data from of devices. Many devices ï including ones from very large manufacturers - are simply incapable of having data removed without additional investments by the provider. Our members find this unacceptable and **do not believe that devices should be approved by the FDA if they are unable to report data out.** Examples of devices which are often stand-alone and do not interoperate with other systems are: bone density; dentistry systems; and ophthalmology systems. Simply knowing whether the device allows data to be moved would be incredibly helpful. Finally, to our earlier point about there being no recourse for a provider who experiences a challenge around interoperability of a device, unless something is contractually obligated, providers may find themselves purchasing a device that does not work as intended.

VI. Recommendations for Contents of Pre-market Submissions

FDA notes that, ñwhen making a claim that a device exchanges and uses information with or from other devices, technologies, or products, the information submitted should be sufficient to support the claim.ò Going back to our earlier concerns about the lack of sufficient recourse for a provider should the device not operate as intended from an interoperability standpoint, having greater ñlabelingòtransparency could help with this.

A. Device Description

FDA calls for manufacturers to, ñAs part of the device description typically submitted in a pre-market submission, sponsor should include a discussion of any electronic data interfaces found on the device, the purpose of each interface, and the anticipated users of the interfaces. Describe how each interface is meant to be used or the limitations of the use of the interfaces. If the interface is only meant to be used by the manufacturer, this should be clearly stated. If the interface is meant to be used with only specific devices, those devices should be clearly specified.ò Again, there is a need for sufficient transparency for those purchasing these devices. Publishing the list of elements listed on lines 537-552 would aid providers in their purchasing decisions. We recommend adding to this list the ability to send data outside of the device without additional intervention needed by a provider (i.e. ability to send data in a standard format to an EHR).

FDA says certain elements should be included as part of this review. CHIME agrees with the way FDA has described the elements that manufacturers should consider and describe in their premarket submissions concerning claims of data exchange.

B. Risk Analysis

Please see our comments under Section V.C.

C. Verification and Validation

Please see our comments under Section V.D.

D. Labeling

Please see our comments under Section V.E.

Conclusion

CHIME appreciates the opportunity to offer perspective. We stand ready to working collaboratively with the FDA and other agencies to improve interoperability. Please contact Mari Savickis, vice president, federal affairs at msavickis@chimecentral.org, with any questions.

Sincerely,

Russell P. Branzell

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Marc Probst, CHCIO
Chairman, CHIME Board of Trustees & CIO, Intermountain Healthcare