HIMSS Electronic Health Record Association

33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@ehra.org
Phone: 312-915-9518
Twitter: @EHRAssociation

AdvancedMD
AllMeds
Allscripts
Aprima Medical Software
BestNotes
Bizmatics
Cerner Corporation
ChartLogic, A Division of Medsphere Systems
CureMD Corporation
eClinicalWorks, LLC
eMDs
EndoSoft
Epic
Evident
Flatiron Health
Foothold Technology
Greenway Health
Harris Healthcare Group
Lumeris
MacPractice
MEDHOST
MEDITECH
Modernizing Medicine
Netsmart
Nextech
NextGen Healthcare
Office Practicum
Sevocity, A Division of Conceptual Mindworks
SRS Health
STI Computer Services
Vālant Medical Solutions
Varian Medical Systems
Virence Health
Wellsoft Corporation

March 26, 2019

The Hon. Mark R. Warner
United States Senate
428 Senate Dirksen Office Building
Washington DC 20510

Dear Senator Warner,

On behalf of the Electronic Health Record (EHR) Association, we are pleased to support your efforts to reduce cybersecurity vulnerabilities in the healthcare sector.

The EHR Association is a trade organization that brings together more than 30 companies that develop, market, and support electronic health records (EHRs), to collaborate on issues that impact their businesses and their collective customers — hospitals and providers that represent the majority of EHR users in the U.S. The Association speaks with a unified voice on health information and technology (IT) issues in a non-competitive, collegial effort to understand, educate, and collaborate with all stakeholders engaged with EHRs and other technologies.

Privacy and security is an area of focus and engagement within the EHR Association's software developer community, along with other stakeholders. As you know, cybersecurity has been a hot topic in the past few years, with considerable work done in both the security sector as a whole and within the healthcare industry. Specific to your intention to "develop a short and long term strategy for reducing cybersecurity vulnerabilities in the health care sector," the Association recommends two resources as starting points for the development of a strategy:

- The Commerce Department's "NIST Cybersecurity Framework."
- HHS's Health Care Industry Cybersecurity Taskforce's "Report on Improving Cybersecurity in the Health Care Industry."

The NIST Cybersecurity Framework is a voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk. In the last five years, the framework has had wide adoption across many sectors, including the healthcare industry, and serves the basis for or shares methodologies with other popular cybersecurity frameworks.

In May 2017, President Trump issued the "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which directs all federal agencies to use the Cybersecurity Framework.

HHS established the Health Care Industry Cybersecurity Taskforce following passage of the Cybersecurity Act of 2015. Taskforce members represented a wide variety of organizations within the healthcare and public health sectors, including hospitals, insurers, patient advocates, security researchers, pharmaceutical companies, medical device manufacturers, health information technology developers, and laboratories.

On June 2, 2017, the Taskforce issued its findings to Congress, in what is known in the industry as the Health Care Industry Taskforce Report ("Report on Improving Cybersecurity in the Health Care Industry"). The Taskforce Report calls for a collaborative public and private sector effort to protect our healthcare systems and patients from cyber threats and to work together to meet this urgent challenge, outlining a national strategy to meet these goals.

This work by the Health Care Industry Cybersecurity Taskforce is a solid starting point for any new work toward a national strategy to reduce cybersecurity threats.

We would also refer you to the Department of Homeland Security's Healthcare Sector Coordinating Council (HSCC), of which the EHR Association is an active member. HSCC's Cybersecurity Working Group is tasked with identifying major cybersecurity threats and vulnerabilities to the security and resiliency of the healthcare sector, and developing cross-sector policy and strategic approaches to mitigating those risks.

Below we're pleased to share our responses to the specific questions in your request for information. In cases where questions are asked at the individual organization level, the Association has responded with recommendations as a trade organization representing a cross-section of member companies. Where appropriate, we have referenced notable works and initiatives that have already gained traction in the security and healthcare industries.

Questions in RFI:

1. ***What proactive steps has your organization taken to identify and reduce its cyber security vulnerabilities?***

To reduce, manage and continually monitor security and privacy risks, the EHR Association recommends that both developer and provider organizations employ a risk-based privacy and security framework based on NIST's Cybersecurity Framework (or others such as ISO 27001/27002, CIS Critical Security Controls, HITRUST, and PCI DSS).

2. ***Does your organization have an up-to-date inventory of all connected systems in your facilities?***

NIST's Cybersecurity Framework includes controls of asset management. This includes guidance on inventorying of devices, systems, software platforms, applications, external information systems. Also, the framework outlines the mapping of organizational communications and data flows, prioritization of resources, and definition of cybersecurity roles and responsibilities.

3. Does your organization have real-time information on that patch status of all connected systems in your facilities?

NIST's Cybersecurity Framework includes controls on software, firmware, and information security that include having appropriately timed patch status on connected systems based on risk.

4. How many of your systems rely on beyond end-of-life software and operating systems?

As an industry, EHR developers encourage customers to keep up with the latest patches and upgrades to any systems used with EHR products. On the occasions that customers rely on end-of-life software and operating systems, we would recommend customers consult their cybersecurity framework.

NIST's Cybersecurity Framework includes a control with guidance on the continued use of information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

5. Are there specific steps your organization has taken to reduce its cybersecurity vulnerabilities that you recommend be implemented industry wide?

The EHR Association encourages member company participation in information sharing organizations — such as the Health-ISAC (H-ISAC), InfraGard, and the Cyber Health Working Group (CHWG) — as a way for healthcare organizations and developers to stay on top of current cyber threats and to prepare for the future. We encourage member companies to share relevant security and privacy information with their customers, including security advisories related to products, recent trends, and best practices.

Though not an exhaustive list, these are specific steps EHR Association member companies may have taken or are recommending to their customers, and/or are directly assisting customers with implementing to help reduce their cybersecurity vulnerabilities:

1. **Cybersecurity Staff:** EHRA member companies recommend that customers dedicate existing staff and/or hire new staff to address cybersecurity. Having dedicated cybersecurity staff is important as they will bring a new and focused perspective to the organization. Cybersecurity is not purely a technology problem, so an effective cybersecurity staff member must be more than a technologist and understand both people and process. Also, cybersecurity staff must be able to raise security awareness within the organization; create

impactful policies and procedures that do not hinder primary business goals; and educate leadership on cybersecurity risks.

2. **Scan the Network:** EHRA member companies recommend that customers scan their network for systems from an external perspective to identify which systems are available from the internet. Scan all systems on a regular basis with the goal of identifying vulnerabilities. Scanning tools come in great variety, but essentially they allow IT (information and technology) staff to be able to identify all systems on their network, and whether or not they are vulnerable.
   a. With the exception of a few servers (web servers, for example), servers should not be accessible from the internet.
   b. In 2017 and 2018, there were a series of very serious ransomware attacks which took down hospitals for several weeks. In many of these cases, the reason the attackers were able to cause so much damage was that they were able to gain remote access to servers.
   c. Because of this, the FBI issued this warning that increasingly the remote desktop protocol (RDP) has been exploited by hackers.
   d. Scanning the organization's network can identify servers which have not been recently patched (that is, updates to the operating system and other software have not been taken) and are therefore vulnerable.

3. **Administrative Accounts on Servers:** EHR Association member companies recommend that customers regularly review administrative accounts on servers, review password policies, and ensure that systems follow the latest NIST password guidelines.
   a. Administrators are those staff which have full access to the server. They are a special target of hackers due to their level of access.
   b. Password policies should be set so that complex and long passwords are required.
   c. Requiring that staff routinely reset their password means that any hackers who know that password will not be able to access the system once it is reset.

4. **SMB Shares:** EHRA member companies recommend that customers scan for Server Message Block (SMB) shares, examine whether or not SMB shares are required or whether or not alternative methods can be used.
   a. SMB is a file sharing system built into Windows and other operating systems. It can be set up so that not everyone has access to a folder with files, and it can also require a password. It is important that critical files are not shared openly on the network.
   b. There was an exploit of SMB called "EternalBlue" which was developed by the NSA and leaked in 2017. This exploit was then used in the WannaCry ransomware and NotPetya malware attacks which caused significant damage in healthcare and other industries:
      i. WannaCry
      ii. NotPeyta
   c. Eliminating use of SMB file shares (where possible) is the best option.
   d. When elimination is not an option, systems should use the most recent version of SMB, which is currently version 3. This most recent version does not have the serious vulnerabilities of versions 1 and 2.

5. **Multi-factor Authentication:** EHR Association member companies recommend that customers, with the help of their developer, implement additional factors of authentication for all critical systems. Rather than relying on just a username and password provide another "factor of authentication" that verifies the user.
    a. Username and password - referred to as "something the user knows."
    b. Biometrics - referred to as "something the user is (fingerprint, handprint, or retina scan)."
    c. A physical device of some kind - this could include a hard token (a USB which is plugged into the computer), a phone (near field communications between the phone and the computer), or even a badge (radio frequency ID or RFID badge, which is waved near an RFID reader). This is referred to as "something the user has."
    d. Onetime password - user receives a onetime password as a text message to his/her phone, or use an authenticator app which generates a string of numbers which must be entered.

6. **Lock down software applications:** EHR Association member companies recommend that customers, with the assistance of their developer, lock down software applications. This would include locking down Microsoft Office Macros to the extent that this is possible without hampering functionality. Macros can be used in a malicious way as an attacker could simply send an MS Word document with a specially created macro which gets launched when the document is opened with macros enabled. Exploiting MS Word macros in this way are a very common method used by hackers.

7. **Collaboration:** EHRA member companies recommend that customers work closely with EHR, medical device, software, and other vendors on best practices for securing all systems.

8. **Create a DMZ:** EHRA member companies recommend that customers create a demilitarized zone (DMZ) for all externally facing servers.
    a. Externally accessible servers are attacked frequently by hackers, which if successful, can be used to attack nearby systems. Servers located in a DMZ cannot easily connect to other servers through the protection of a firewall.
    b. Externally facing virtual machines (VMs) should not be on the same host as internal VMs, as this would prevent hackers from being able to successfully take over other VMs.

9. **Network Segmentation:** EHR Association member companies recommend that customers create separate network segments for user devices, guest devices, medical devices, servers, etc. Firewalls should be used to restrict communication between network segments. Typically hackers can gain access to end user devices quite easily via phishing email and malicious websites. By segmenting networks, hackers will have difficulty gaining access to more critical devices (such as servers and medical devices). Network segmentation is similar to having separate rooms--i.e., one room for end user devices and another room for servers--separated by locked doors.

10. **Administrator Account Management:** EHR Association member companies recommend that customers use Microsoft LAPS (in Windows environments; this is free) to manage local administrator passwords on all end user devices. Administrator accounts are necessary so that IT support staff can service devices (i.e., install software, update the operating system) and the use of LAPS makes lateral movement within an organization more difficult for hackers.

11. **Patch Systems Regularly:** EHR Association member companies recommend that customers update their software regularly. New exploits are found frequently, and software companies provide regular "patches" or updates to their software. In most cases, these are provided once a month. These patches require system administrators to test and move the updates to all of the systems on their network. Many healthcare organizations patch far less frequently than needed because they cannot dedicate the time to take down critical systems for the update or a fear that an update may cause systems to "break."

12. **Intelligence Feeds:** EHR Association member companies recommend that customers subscribe to the United States Computer Emergency Readiness Team (US-CERT), CHWG, H-ISAC, and other intelligence feeds pertaining to the technologies in use. For example, Cisco and Microsoft have blogs and technical security notification services.

13. **Penetration Tests:** EHR Association member companies recommend that customers perform penetration testing of networks and systems. A penetration tester is someone who attacks the network and systems with the same tools and manner as a hacker.
    a. The penetration tester may be an employee of the organization, who regularly does this kind of attacking, or it may be someone from a security firm who is brought in to attack the systems on a regular basis (often once or twice a year).
    b. This should include physical security testing as well, since good information security depends on the security of data centers, network jacks, and more. In a physical penetration test, the tester may try various methods to gain physical access to locations and equipment.

14. **Security Awareness:** EHR Association member companies recommend that customers regularly (monthly) provide useful information about security and privacy to all staff. Include items that are relevant for both work and personal life.

15. **Insider Threat:** EHR Association member companies recommend that customers create an insider threat program. Insiders may steal information, medications, or spy on medical records of family members, neighbors, or celebrities. Because insiders have access to systems, it can be difficult to spot a malicious or curious insider. Organizations should take the following actions:
    a. Regularly review audit logs.
    b. Consider a third party solution which filters through audit logs and identifies suspicious staff activity.

16. **Train Privileged Users:** EHR Association member companies recommend that customers provide annual training on security practices to privileged users (i.e. administrators) because they are specifically targeted by hackers.

17. **Develop Business Continuity, Disaster Recovery, and Incident Response plans:** EHR Association member companies recommend that customers work within their respective organizations to create, document, and test these plans. Plans should include developing and practicing "back to paper" procedures for all staff.

18. **Secure Email Systems:** EHR Association member companies recommend that customers take action to secure email systems. Phishing is still an extremely effective and inexpensive threat. Organizations should consider the following:
    a. Implement technologies (SPF, DKIM, and DMARC) that prevent hackers from sending emails that appear to originate from the organization's own email system (also known as "spoofing").
    b. Implement spam filtering to remove most unwanted email from users' inboxes.
    c. Scan all email attachments for malicious threats.
    d. Add warnings to emails which originate from outside the organization.
    e. Secure email servers if on premise using NIST guidelines.
        i. NIST SP 800-177 - Trustworthy Email
        ii. NIST SP 800-45 - Guidelines on Electronic Mail Security

19. **Backup Critical Systems:** EHR Association member companies recommend that customers create backups as an important strategy to ensure resilience. Backups allows an organization to restore systems in the event that a server is destroyed (i.e., electrical surges, flooding, ransomware). Organizations should consider the following:
    a. Develop a comprehensive backup strategy that includes the EHR system as well as local, end user devices which may have a variety of essential software.
    b. Protect backups using guidance from the CIS Critical Security Controls for Effective Cyber Defense Version 6.1 (available for download from the CIS website here).
    c. Validate and test backups on a regular basis.
    d. Use the 3-2-1 rule as defined here by US-CERT.

20. **Security Incident Response (IR) Firm:** EHR Association member companies recommend that customers have a security incident response firm on retainer. Contracts need to be established well in advance of a cyber-attack.

21. **Develop Relationships with Law Enforcement:** EHR Association member companies recommend that customers build relationships with local, state, and federal law enforcement. Established relationships lead to increased communication and coordination during a crisis. Additionally, law enforcement provides threat intelligence and guidance freely to public and private organizations.

22. **Manage Third Party Risk:** EHR Association member companies recommend that customers implement a third party risk management program. A good third party risk management program will investigate the security of third party vendors and, depending on the information provided by the third party vendor, put additional controls in place to protect the organization from the third party.

23. **Cloud Hosted Solutions:** EHR Association member companies recommend that customers using cloud hosted solutions consider the following (not an exhaustive list):
    a. Establish a Business Associate Agreement (BAA). Not all cloud providers will sign a BAA, so we advise this be discussed early in the procurement process.
    b. Clear documentation on responsibilities during a security incident, including access to audit logs, law enforcement notification, etc.
    c. Assurances on the security of the cloud hosted solution (e.g., SOC audits, certifications such as ISO 27000, data center certification, etc.).
    d. Service Level Agreements (SLAs) - including a clear understanding of any penalties for systems being down over a period of time.
    e. Business Continuity/Disaster Recovery - including a clear understanding of the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
    f. Compliance with all applicable state and federal regulations.
    g. While the cloud itself may be more secure and reduce risk, the covered entity will need to carefully consider a variety of security controls including user authentication, access control, secure access to the cloud, and activity monitoring.

6. ***One of the imperatives from the Health Care Industry Cybersecurity Task Force Report is for the sector to "develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities." To that end, what workforce and personnel challenges does your organization face in terms of security awareness and technical capacity? What steps have you taken to develop the security awareness of your workforce and/or add or grow technical expertise within your organization?***

The EHR Association recognizes the lack of trained privacy and security professionals in health IT and supports the development of cybersecurity-focused leadership and workforce at all organizations -- i.e., government agencies, healthcare organizations, and health IT developers. EHRA recommends such entities work closely with local colleges and universities to develop cyber talent, in addition to providing time and opportunities for their own staff to pursue further education toward industry accepted certifications such as — but not limited to — Security+, Certified Ethical Hacker (CEH), and CISSP.

7. ***Has the federal government established an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector? If not, what are your recommendations for improvement?***

The Health Care Industry Cybersecurity Task Force and its report comes to mind as a national strategy to reduce cybersecurity vulnerabilities in the healthcare sector. However, from our understanding, the strategy has not been implemented by the federal government. We recommend that the federal government review and consider implementing the recommendations and imperatives outlined as a starting point for developing a national strategy, which should encourage and/or incentivize organizations to attest to recognized programs such as HITRUST CSF, or SOC.

8. ***Are there specific federal laws and/or regulations that you would recommend that Congress consider changing in order to improve efforts to combat cyberattacks on health care entities?***

Because inconsistencies in state and federal privacy laws pertaining to sensitive health information are obstacles to privacy and security of health systems, the EHR Association supports efforts to harmonize state and federal regulations affecting cybersecurity of health information and technology.

We strongly caution that there is a difference between compliance and security. As Kevin Magee (formerly on the Board of Brant Community Healthcare System) stated, “Compliance is that I use the crosswalk when I cross the street. Security is that I look both ways before I step out.”

Regulation can have a beneficial impact on behavior, but it does not guarantee security. Healthcare systems need to hire cyber talent and put in place processes and procedures — such as patch management and scanning for vulnerabilities and open systems — that will *maintain* the security of their systems.

Addressing barriers to healthcare IT security collaboration would help further the security of the industry. While Stark regulations contain exemptions for sharing an EHR (42 CFR 411.357), there is not an exemption for IT services such as cybersecurity. Healthcare organizations which depend on the EHR exemption for access to an EHR may also lack the resources to recruit, manage, and fund the expertise and tools needed to prevent cyber-attacks. Finding new ways to incentivize the adoption of critical security controls should be evaluated to help accelerate the reduction of cybersecurity vulnerabilities in the industry.

9. ***Are there additional recommendations you would make in establishing an industry wide strategy to improve cybersecurity in the health care sector?***

First, we’ll reiterate the work already done by the HHS Health Care Industry Cybersecurity Taskforce and recommend that any new work establishing an industry wide strategy start with the Taskforce report.

Second, the EHR Association recognizes that the majority of healthcare-related cybersecurity breaches are due to a lack of privacy and security best practices at both the IT administration and end user level. To improve this, we encourage the development of programs that provide awareness and basic education on cybersecurity best practices for health professionals, and development of a culture that sees privacy and security as an enabler of improved patient trust and better health outcomes.

Furthermore, we recommend the Office of the National Coordinator for Health IT’s (ONC) *Guide to Privacy and Security of Electronic Health Information* as a primer for healthcare organizations and individual professionals to understand how to comply with privacy and security policy requirements.

Third, the Association recognizes that reducing cybersecurity risk is a complex problem and not every organization in the healthcare domain has the resources available to reduce its risk. Some organizations face financial hardships (especially smaller providers such as small community hospitals and small practices) and do not have access to trained cybersecurity staff nor financial resources to implement a cybersecurity program. A federal program that provides financial assistance to healthcare organizations for cybersecurity improvements such as, but not limited to, education, staff, and infrastructure, would help.

Fourth, though we strongly recommend the use of the NIST Cybersecurity Framework, we recognize that implementation of the NIST Framework (or any framework) is not straightforward for organizations at all levels of the healthcare industry. We encourage the development of implementation guides and best practices to apply the Framework, specific to the many facets of healthcare and health IT, to facilitate and improve adoption.

Fifth, everyone in the healthcare industry must understand that cybersecurity is a patient safety issue, requiring the unified efforts of clinical, IT, and business staff to properly address.

Some organizations view cybersecurity only in terms of financial risks, with security seen as a cost by most organizations. Proper viewpoint is essential. For example, ransomware has severely impacted some hospitals, but the threat has not been so prevalent that it could financially justify the budget required to prevent it. When viewed as a serious threat to patient safety, however, it becomes clear that additional expenditures are justified.

Thank you for this opportunity to share our expertise. We're grateful for your leadership on this issue and look forward to continuing to work with you to ensure the safety, resilience, and security of our nation's healthcare industry.

Should you or your staff wish to discuss our recommendations in more detail, please contact Sarah Willis-Garcia, EHRA Program Manager, at swillis@ehra.org or 312-915-9518.

Sincerely,

Cherie Holmes-Henry

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Sasha TerMaat

Sasha TerMaat
Vice Chair, EHR Association
Epic

HIMSS EHR Association Executive Committee

Dal J Bucciferro

David J. Bucciferro
Foothold Technology

Hans J. Buitendijk
Cerner Corporation

Barbara Hobbs

Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
Evident

Emily Richmond

Emily Richmond, MPH
Allscripts/Practice Fusion

Courtney E Tesvich

Courtney E. Tesvich, RN
Nextech

About the EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.