HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

October 26, 2018

Susan Edwards
Associate Counsel
Office of Inspector General
Department of Health and Human Services
Attention: OIG-0803-N
Room 5513, Cohen Building
330 Independence Avenue, SW
Washington, DC 20201

Dear Ms. Edwards:

The Healthcare Sector Coordinating Council (HSCC) is pleased to comment on, "Medicare and State Health Care Programs: Fraud and Abuse; Request for Information Regarding the Anti-Kickback Statute and Beneficiary Inducements CMP," published in the *Federal Register* on August 27th.

The HSCC is a private sector-led advisory council of major health industry stakeholders working together and with the U.S. Department of Health & Human Services (HHS) to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to the nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents more than 200 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology (health IT), health plans and payers, laboratories, and biologics and pharmaceuticals. Our members collaborate to improve the cyber security and resiliency of the healthcare industry and improve patient safety. Our members are responsible in different capacities for protecting and securing patient information, something that is fundamental to spurring a healthcare system that is driven by value rather than volume.

We appreciate the opportunity to lend our voice to this policy discussion and recognize that a Request for Information (RFI) is a preliminary fact-finding step undertaken by an agency to begin soliciting stakeholder feedback aimed at shaping potentially forthcoming regulation. We also recognize that the Office of the Inspector General (OIG) is seeking input on the broader question of removing regulatory barriers to care coordination, but we have limited our comments to how OIG can take steps to improve cybersecurity in healthcare.

Overarching Feedback

Based upon our review of the RFI our topline feedback is:

1. **Cybersecurity threats pose a significant risk to patient safety;**
2. **We recommend OIG create a waiver under the Anti-kickback rules that allows for the donation of cybersecurity technology and services to help improve the cybersecurity posture of providers, better protect patient information, improve patient safety, encourage secure data exchange, and help fortify our sector from growing global threats; and,**

3. **In creating such an exception, we recommend OIG work with public and private sector subject matter experts to develop a specific definition of cybersecurity technology**

Patient Safety

Cybersecurity threats pose a risk to patient safety, an issue that has been recognized by the Food and Drug Administration (FDA) and was described as such by the FDA Commissioner in a recent statement.[1] And, a key finding in a report[2] published October 5th by KLAS Research on medical device security revealed that patient safety is a top concern for providers.

A number of recent studies have concluded cybersecurity vulnerabilities have potentially compromised patient care. A recent study by University of California Cyber Team concluded that patients are being harmed from "compromised healthcare infrastructure cybersecurity events, like ransomware, malware, compromised EHRs or an attack on facility systems."[3] And, recent research coming out of Vanderbilt that relied on data from the U.S. Department of Health & Human Services (HHS) found that data breaches are tied to patient deaths.[4]

As the healthcare system has become more digitized and payment policies necessitate the use of vast quantities of data to drive value and avert financial penalties for not exchanging information, providers are increasingly vulnerable to the ever-growing number of cybersecurity threats. According to the Department of Homeland Security's (DHS) 2018 Cybersecurity Strategy, "Enabling the delivery of essential services—such as electricity, finance, transportation, water, and health care—through cyberspace also introduces new vulnerabilities and opens the door to potentially catastrophic consequences from cyber incidents. The growing number of Internet-connected devices and reliance on global supply chains further complicates the national and international risk picture."[5]

As we have noted in our response[6] to the Centers for Medicare & Medicaid Services (CMS) RFI on suggested modifications to Stark Law regulations, we request you consider the following statistics:

- The healthcare industry is the target of twice as many cyber-attacks as other industries.[7]
- Over 80 percent of physician practices report they have experienced a cyberattack.[8,9]

---

[1] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm

[2] https://klasresearch.com/report/medical-device-security-2018/1471

[3] https://www.healthcareitnews.com/news/security-risk-storm-here-medical-device-threats-are-real-and-patient-safety-risk

[4] https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/07/WEIS_2017_slides_2.pdf

[5] https://www.dhs.gov/publication/dhs-cybersecurity-strategy

[6] https://healthsectorcouncil.org/wp-content/uploads/2018/08/SCC-JCSWG-Policy-group-comments-on-Stark-RFI-vFINAL-v2.pdf

[7] https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

[8] http://365.himss.org/sites/himss365/files/365/handouts/550400807/handout-255.pdf?_ga=2.88126555.1717737500.1534339704-1399426361.1511991976

[9] https://www.ama-assn.org/sites/default/files/media-browser/public/government/advocacy/infographic-medical-cybersecurity.pdf

- Healthcare breaches continue to grow with an average of one a day occurring in 2017[10] and 2018 is on track to be the highest year ever.
- Healthcare data fetches much more money on the black market than other personal data–sometimes hundreds or thousands of dollars[11]-and the Federal Bureau of Investigation (FBI) has said connected devices are at risk for increased cyber intrusions for financial gain.[12]
- According to KLAS Research, the average number of connected devices across providers of various sizes is 10,000.

Fortifying Healthcare Sector's Cyber Posture Will Help Drive Value

The Federal Anti-kickback statute provides criminal penalties for individuals or entities that knowingly and willfully offer, pay, solicit, or receive remuneration to induce or reward the referral of business reimbursable under Federal healthcare programs. To help accelerate the transformation to a value-based system that includes care coordination, HHS launched a "Regulatory Sprint to Coordinated Care" focused on identifying regulatory provisions that may act as barriers to coordinated care; assessing whether those regulatory provisions are unnecessary obstacles to coordinated care; and issuing guidance or revising regulations to address such obstacles and, as appropriate, to encourage and incentivize coordinated care while protecting against harms caused by fraud and abuse.

The widespread growth of data sharing in healthcare presents increased threats of patient data compromise and potential risks to patient safety. Given the volume of data exchange needed to foster a system that is oriented around value rather than volume, helping healthcare entities ensure the data with which they have been entrusted by patients is safeguarded will serve the healthcare industry well. Therefore, regulatory policies that support the ability of healthcare entities to better protect patient data are needed. This need is particularly acute for small to mid-sized healthcare providers that do not have the resources or expertise to secure systems and data against cybersecurity threats and vulnerabilities or fend off cybersecurity attacks. It is important to note that the American Medical Association reports that only one in five small physician practices have an in-house security official.

OIG recognizes that cybersecurity threats are a top management challenge to HHS and identifies fostering a culture of cybersecurity beyond HHS as a key component for protecting beneficiaries.[13] Moreover, OIG recently formed a multidisciplinary Cybersecurity Team comprised of auditors, evaluators, investigators, and attorneys focused on combatting cybersecurity threats within HHS and the healthcare industry. Furthermore, OIG calls on HHS to use policy levers to encourage cybersecurity efforts without creating undue burden. The OIG should use its own policy lever by issuing a safe harbor to promote cybersecurity throughout the healthcare system.

[10] https://www.hipaajournal.com/healthcare-data-breaches-in-2017/

[11] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#d42601650cf1

[12] https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf

[13] https://oig.hhs.gov/reports-and-publications/top-challenges/2017/2017-tmc.pdf#page=45

The growth of digitized medicine and connected devices has opened the doors for those intent on wreaking havoc and stealing and exploiting patient data with increasingly sophisticated methods. Most providers are ill-equipped to combat cyberattacks, especially attacks by nation states and criminals.

Recent Global Attacks Wake Up Call

Cyberattacks such as Petya and WannaCry brought widespread attention to the myriad of cybersecurity vulnerabilities in the healthcare sector and demonstrated the importance of improved preparedness and rapid response in the event of an incident. According to a recent article in the *New England Journal of Medicine*, the WannaCry cyberattack presents a "wake up call" to the American healthcare sector. The United Kingdom's National Health Service (NHS) was crippled from the attack in 2017 when a hospital employee opened an infected email, launching what amounted to a ransomware attack, throwing their system into chaos, and interrupting care for a substantial number of British citizens. This attack spread to more than 150 countries and affected more than 200,000 computers across the globe and the vulnerability is still spreading. On the heels of WannaCry, other global attacks followed. The subsequent Petya attack took control of computers and demanded ransom in Bitcoin, affecting hospitals in at least two states and a pharmaceutical company in the U.S.

Recommendations by Cybersecurity Industry Task Force

The Cybersecurity Industry Task Force Report,[14] mandated by the Cybersecurity Information Sharing Act of 2015 (CISA), includes more than one hundred recommendations on how the healthcare sector can improve its cyber posture. The report includes a discussion (page 35) on the various issues associated with the Anti-kickback and Stark statutes. The report says:

> *A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHR) effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cybersecurity provision. Physician groups confront a myriad of financial challenges. Often these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute.*

Creating a waiver under the anti-kickback rules that allows for the donation of cybersecurity technology (both hardware and software), training, and tools to providers (i.e. under-resourced or less sophisticated ones) will improve the overall cybersecurity posture of our industry and will help guard against cyberattacks that threaten patient safety.

OIG Q's & A's

Q. **How might such items or services reduce cybersecurity risks to the following: The donor, the recipient, patients, and other nonparties to the arrangement?**

[14] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

A. As described above, sharing cybersecurity items and services would likely help mitigate potential risks to patient safety by fortifying the cybersecurity posture of as many healthcare organizations and practices as possible. In particular, smaller and lesser-resourced providers need help enhancing their cyber posture. The security of the healthcare system is only as strong as its weakest link, so it would benefit the entire healthcare industry to support the provision of cybersecurity resources outside of large health systems. Doing so would help to protect a community's larger systems, as well as, the affiliated small and medium-sized practices.

Q. Are there technical or legal barriers (besides the physician self-referral law and the anti-kickback statute) that could prevent or limit the arrangements?

A. Since technology is always evolving (i.e. updates / patches), we recommend OIG account for the need that the method to protect the technology must change and not be hampered by the spirit of the anti-kickback statute. Providers have an on-going obligation to protect the technology and safely provide patient care. In many cases, the technology (or accompanying security updates/fixes) would not be a one-time donation but something that would need to be maintained over time, particularly in the case of hardware and software. Further, feedback from many providers suggests that the anti-kickback rules are getting so complicated that providers are avoiding contracting with others to provide security out of fear of violating the anti-kickback rules. The patient care relationships providers enter are based on patient safety. Therefore, while security may be a factor informing this decision it should not be a factor in failing to establish a care coordination relationship.

Additionally, conducting cybersecurity research among stakeholders requires navigating a daunting and very complicated legal landscape, especially for the provider. The legal complexity – the most complicated of which are the OIG's AKS rules – present substantial challenges that prevent providers, manufacturers, IT infrastructure vendors, and others from working collaboratively together to develop test beds for the purposes of detecting and defending against future cyberattacks and learning from previous ones. While the FDA is working with MITRE on a pilot that attempts to address these issues, the legal complexities for the participating provider were daunting. The challenges for a smaller or mid-sized provider in overcoming these would be nearly impossible given the extreme challenges faced by larger and better resourced providers.

Q. Are there any potential risks or unintended consequences to such arrangements (e.g., potential for fraud or abuse, information blocking, or anti- competitive practices) and, if so, how might these risks be mitigated? Are there any particular risks if HHS takes no action?

A. In the absence of such a waiver, providers – especially those serving medically underserved areas and populations (MUA/Ps)–will continue to struggle to keep pace with the threat environment which is growing daily and becoming increasingly more sophisticated.

Another challenge if OIG does not allow these types of donations is that it could hamper the exchange of data and interoperability which could run afoul of current and forthcoming data blocking prohibitions. Providers have an obligation to know who they share data with and that the data shared is protected. Allowing providers to share or

pool security resources helps build this trust and therefore would aid the exchange of data and interoperability. Thus, by allowing the better resourced providers to help the smaller or lesser resourced ones, this will ultimately better facilitate interoperability and data exchange.

Conclusion

The HPH SCC JCWG Policy Working Group appreciates the opportunity to comment on this important issue and urges the agency to identify as many incentives as possible to help providers safeguard patient data to guard against these growing threats.

Sincerely,

Greg Garcia
Executive Director for Cybersecurity
Healthcare Sector Coordinating Council