August 24, 2018

The Honorable Seema Verma
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Administrator Verma:

As co-chairs of the Policy Task Group of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cyber Security Working Group (CWG), composed of 198 healthcare organizations, companies and associations from across the healthcare industry, we are pleased to comment on behalf of the majority[1] of the HSCC CWG members on the Centers for Medicare and Medicaid Services' (CMS), "Medicare Program; Request for Information Regarding the Physician Self-Referral Law," published in the *Federal Register* (83 FR 29524) on June 25, 2018.

We appreciate the Administration's efforts to reduce regulatory burdens on healthcare providers. The organizations representing the HSCC span the health care sector and have a vested interest in advancing the cyber posture of the healthcare industry and improving patient safety. Our members are responsible in different capacities for protecting and securing patient information, something that is fundamental to supporting a healthcare system that is driven by value rather than volume. **We recommend CMS create a Stark exception that allows for the donation or subsidizing of cybersecurity technology and services to help improve the cybersecurity posture of providers, better protect patient information, improve patient safety, and help fortify our sector from growing global threats.** In creating such an exception, we recommend CMS work with subject matter experts to develop a specific definition of cybersecurity technology.

Stark Rules Outdated for Today's Electronic & Connected Environment

The physician self-referral statute (Stark Law) and its implementing regulations were enacted prior to the development of information technologies that improve the efficiency and quality of the Medicare and Medicaid programs. Since that time, the healthcare system has evolved into a vastly different network that is heavily dependent upon data being stored and moved electronically. Today's environment continues to rapidly change as technology evolves and new challenges have arisen since the law was first enacted. Consider also the following statistics:

[1] 40 member organizations of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cyber Security Working Group (CWG) approved, 1 abstained and 2 opposed

- The healthcare industry is the target of double the number of cyberattacks as other industries.[2]
- Most physicians have experienced a cyberattack.[3,4]
- Healthcare breaches continue to grow with an average of one a day occurring in 2017[5], 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[6] and the Federal Bureau of Investigation has said medical devices are "at risk for Increased Cyber Intrusions for Financial Gain."[7]
- According to KLAS Research the average number of connected devices across providers of various sizes is 10,000.

Attacks have become more sophisticated, the growth of digitized medicine and connected devices has expanded the threat vector for those intent on disrupting hospital systems, stealing and exploiting patient data. Most providers are ill-equipped to combat cyberattacks, especially sophisticated attacks by nation states and criminals. Of critical importance is that these risks pose serious threats to patient safety, a threat that has been recognized by the Food and Drug Administration (FDA). In fact, a recent study by University of California Cyber Team concluded that patients indeed are being harmed by compromised medical devices.[8] Moreover, 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.[9]

As the healthcare system has become more digitized, CMS policies mandating data exchange and interoperability have increased in scope, and the use of mobile apps and connected medical devices has proliferated the ability of many providers to keep up with the ever-growing number of cybersecurity threats is outpaced. According to the Department of Homeland Security's (DHS) 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."[10]

Recent Global Attacks Wake Up Call

---

[2] https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html
[3] http://365.himss.org/sites/himss365/files/365/handouts/550400807/handout-255.pdf?_ga=2.88126555.1717737500.1534339704-1399426361.1511991976
[4] https://www.ama-assn.org/sites/default/files/media-browser/public/government/advocacy/infographic-medical-cybersecurity.pdf
[5] https://www.hipaajournal.com/healthcare-data-breaches-in-2017/
[6] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#d42601650cf1
[7] https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf
[8] https://www.healthcareitnews.com/news/security-risk-storm-here-medical-device-threats-are-real-and-patient-safety-risk
[9] https://medcitynews.com/2018/03/hospital-data-breaches-tied-patient-deaths/
[10] https://www.dhs.gov/publication/dhs-cybersecurity-strategy

Attacks 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 presented 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 ransomware code that threw their system into chaos and interrupted care for an untold number of British citizens. This attack spread to more than 150 countries and infected more than 200,000 computers across the globe, and the vulnerability is still spreading. On the heels of this attack followed other global attacks. The Petya attack that followed months later took control of computers and demanded ransom in bitcoin, affecting hospitals in at least two states and a pharmaceutical company in the U.S. Early in 2018 the Spectre attack was made public, and, like Petya, involved vulnerabilities with chips found in just about every computer and that can be exploited.

Recommendations by Cybersecurity Industry Task Force

The Health Care Industry Cybersecurity Industry (HCIC) Task Force Report[11], mandated by the Cybersecurity Information Sharing Act of 2015 (CISA), includes more than hundred recommendations for how the healthcare sector can improve its cyber posture. The report includes a discussion (page 26) on the various issues associated with the anti-kickback and Stark statutes. "Recommendation 1.5" of the task force report called for:

> *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 Stark exception that allows providers to donate cybersecurity technology (both hardware and software), training and tools to other 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. Cybersecurity risk management in the health sector cannot succeed if enterprises are only able to act independently. As the healthcare system is an interconnected and interdependent network, cyber threats are a shared challenge and a shared responsibility, which requires a team effort.

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

If CMS does not have the ability to create such a Stark exception, we encourage CMS to seek the statutory authority from Congress to create an exception to allow for the donation or subsidy of cybersecurity technology.

Conclusion

The HSCC CWG 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,

Carl Anderson, Chief Legal Officer & SVP Government Affairs, HITRUST
Co-Chair, HPH SCC JCWG Policy Working Group

Theresa Meadows, CIO
Cook Children's Hospital
Co-Chair, HPH SCC JCWG Policy Working Group

Mari Savickis, VP, Federal Affairs, College of Healthcare Information Management Executives
Co-Chair, HPH SCC JCWG Policy Working Group