Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

## Patient Safety Would Benefit from Cybersecurity Exception to Anti-Kickback Statute for National Cyber Security Awareness Month

Since the start of the 2018 summer, the Department of Health and Human Services (HHS) has queried the healthcare industry about how its regulatory structure can be improved to ensure better patient care, including how policy can encourage and incentivize better cybersecurity as an element of patient safety. The Health Sector Coordinating Council – the cross-sector industry advisory body that partners with the government on strategic critical infrastructure protection issues - has raised its hand to respond to these HHS requests, most recently in a letter to the Office of the Inspector General (OIG) RFI on the Anti-Kickback Statute, which makes it illegal for providers to accept bribes or other forms of remuneration in return for generating Medicare, Medicaid or other federal health care program business.

The OIG posed these key questions in their request for information:

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

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

3. 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? d. Are there any particular risks if HHS takes no action?

To summarize the health sector's point of view about how the Anti-Kickback statute impedes progress toward better cybersecurity across the healthcare ecosystem, the HSCC offers the following feedback:

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 subject public and private sector matter experts to develop a specific definition of cybersecurity technology.

<u>This is our Wake-Up Call for Patient Safety</u>

Recent global cyberattacks bring the cybersecurity concerns of the healthcare industry to the forefront, after being in the background of our healthcare security long enough for cyber threat actors to recognize and exploit our vulnerabilities. Cyberattacks such as Petya and WannaCry brought widespread attention to the myriad of cybersecurity vulnerabilities in the healthcare sector. These attacks spread to more than 150 countries and affected more than 200,000 computers across the globe, as well as

hospitals in at least two states and a pharmaceutical company in the U.S. The impact and fallout of these attacks demonstrated the importance of improved preparedness and rapid response in the event of an incident.

As we scan the regulatory horizon for outdated regulations that inhibit our ability to be prepared for and respond to such cyberattacks, the HSCC posed the following observations to HHS about the Anti-Kickback Statute:

1. The healthcare industry is an interconnected ecosystem in which risk is distributed and indiscriminate.
2. Sharing cybersecurity intelligence, capabilities and services would help mitigate potential risks to patient safety by fortifying the cybersecurity posture of as many healthcare organizations and practices as possible.
3. Smaller and lesser-resourced providers especially need help enhancing their cyber posture. The security of the healthcare system is only as strong as its weakest link.
4. Technology is always evolving, therefore OIG should recognize providers have an on-going obligation to manage medical technology, protect information systems and data, and safely provide patient care.
5. A anti-kickback rules are getting so complicated that providers are avoiding contracting with others to provide security out of fear of violating the rules.
6. In the absence of such a cybersecurity safe harbor, providers – especially those serving medically underserved areas and populations (MUA/Ps)–will continue to struggle to keep pace with the threat environment.
7. If a safe harbor is not created, there will continue to be limitations on data exchange and interoperability that could run afoul of current and forthcoming data blocking prohibitions.

The Health Sector applauds HHS for its continuing attention to evolving cybersecurity threats against our critical health infrastructure and patient safety, and how the agency, Congress and the sector can modernize a policy environment that will strengthen our collective inoculation against these threats. In a world where hacking the computer system can be the same as hacking the human, we need to be as concerned about cyber viruses as we are about human viruses.