Government Resources to Help with Cybersecurity

The federal government offers several free resources to help health care entities enhance their cybersecurity. A compilation of these resources is available here.

Additionally, the US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides a free objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational / business networks. You can contact them at: vulnerability_info@cisa.dhs.gov.

Cyber Hygiene Services

The Cybersecurity and Infrastructure Security Agency (CISA) offers several free scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. These services are performed by CISA's highly trained information security experts and can include specific assessments such as:

- Vulnerability Scanning: Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- Web Application Scanning: Evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- Phishing Campaign Assessment: Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- Remote Penetration Test: Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open-source information.

We recommend that practices explore the CISA free scanning and vulnerability assessment services. More information on free cyber hygiene services is available here.

Stark Law and Anti-Kickback Statute Protections for Cybersecurity Technology

The Department of Health and Human Services' Office of Inspector General ("OIG") and the Centers for Medicare & Medicaid Services ("CMS") have codified Anti-Kickback Statute ("AKS") safe harbor and Stark Law exceptions permitting stakeholders to donate cybersecurity technology and services to entities with which they interact. These exceptions define "cybersecurity technology" and explain who is permitted to be a donor and a recipient under the exceptions as follows:

> Definition of "cybersecurity technology": Such technology includes any software, hardware, or other types of information technology.

Protected Donors: At this time, the exceptions to not restrict the types of individuals and entities qualifying for protection under the safe harbor and exception.

Permitted Recipients: The exceptions protect donations of cybersecurity technology and services to any individual or entity without limitation, even if the recipient is a patient.

Recipient Contribution: Given the wide variety of cybersecurity technology and services that may be provided, it is often not practical to require a minimum contribution from recipients; (ii) the cybersecurity safe harbor/exception includes other conditions that prevent abuse or potential anti-competitive behavior; and (iii) donors are still free to require recipients to contribute to the cost of the technology or services provided.

For additional information about this and other recent Stark/AKS changes, please see our AMA resource here.