Reporting and Monitoring Cyber Threats

February 2017

The nation's health care system is part of the national infrastructure that has increasingly come under attack from cyber threats. One of the keys to combatting these cyber threats is for the government, the private sector, and international network defense communities to collaborate and share information. The National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security is responsible for "operat[ing] at the intersection of government, private sector, and international network defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response, mitigation, and recovery efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains." One of the NCCIC's four branches is the United States Computer Emergency Readiness Team (US-CERT) which develops timely and actionable information on threats to the federal and state governments, critical infrastructure owners, international organizations, and private industry. US-CERT also responds to cybersecurity incidents and analyzes data it collects itself and from partners about emerging cyber threats.

US-CERT is in a unique position to inform covered entities and business associates about their cybersecurity efforts as well as benefit from information sharing when a covered entity or business associate experiences a cybersecurity incident. Covered entities should report to US-CERT any suspicious activity, including cybersecurity incidents, cyber threat indicators and defensive measures, phishing incidents, malware, and software vulnerabilities. OCR has provided additional details on appropriate cybersecurity information on its website (https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/), and the US-CERT provides secure forms for reporting all of these types of activities at https://www.us-cert.gov/report/. This type of information sharing is one of the many opportunities for information sharing to protect the entire health care system from cybersecurity threats.

Covered entities and business associates should also monitor the US-CERT website for reports on vulnerabilities. Alternatively, information can be received directly via email by visiting US-CERT's Mailing Lists and Feeds webpage at https://www.us-cert.gov/mailing-lists-and-feeds/. Subscriptions are available to all users for Weekly Vulnerability bulletins, Technical Alerts, Current Activity Entries, and Tips. These subscriptions provide up-to-date information on new vulnerabilities and risks as well as patches and mitigations when available. Covered entities and business associates can leverage this information as part of their Security Management Process

under HIPAA (see 45 CFR § 164.308(a)(1)) to help ensure the confidentiality, integrity and availability of electronic protected health information.

As a recent example, the NCCIC reported on a cyber-threat relative to the healthcare industry: Enhanced Analysis of the Grizzly Steppe Activity. The report provides specific signatures and recommendations to detect and mitigate threats from Grizzly Steppe actors, defend against webshell attacks, and defend against spear phishing attacks. This is just one example of the timely and actionable information that covered entities and business associates can receive by monitoring US-CERT's website or signing up for its email lists or feeds.

Resources:

Department of Health and Human Services, Office for Civil Rights (OCR)
https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html