DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850

Center for Clinical Standards and Quality/Survey & Certification Group

Ref: S&C: 17-17-ALL

DATE: **January 13, 2016**

TO: State Survey Agency Directors

FROM: Director
Survey and Certification Group

SUBJECT: Recommendations to Providers Regarding Cyber Security

Memorandum Summary

- **Recommendations for Providers and Suppliers for Cyber Security:** The Centers for Medicare & Medicaid Services (CMS) is reminding providers and suppliers to keep current with best practices regarding mitigation of cyber security attacks. We have outlined resources to assist facilities in their reviews of their cyber security and IT programs.

Background

The Cybersecurity Act of 2015, section 405(b) required the Department of Health and Human Services (HHS) to develop a report on the preparedness of HHS and health care industry stakeholders in responding to cybersecurity threats. This report is known as the U.S. HHS Preparedness Report and outlines the HHS components responsibilities for cyber security. However, the report does not outline mechanisms for States and facilities regarding procedures to take to protect themselves from adverse cyber events.

In 2016, multiple cyber-attacks occurred worldwide, which included banks, health systems, academia and social media. For example, the website of Health Solutions, one of the largest diagnostic laboratories in India, which was breached by hackers accessing a database that included no less than 35,000 medical records, including HIV reports for registered patients. In the United States, several hospitals and health care providers experienced cybersecurity attacks, commonly known as *Ransomware.* This cyber-attack's motive is primarily financial, with a demand for Bitcoins (an Internet Monetary System) in exchange for restoration of temporarily disabled IT systems, including electronic medical records; paging systems and other IT infrastructure.

Ransomware is just one form of the varied threats to healthcare IT systems. Further, *Ransomware* revealed what is commonly known as Zero Day, a new virus variant where the infection could not have been prevented as there were no existing remedies. Unlike many cyber threats such as stolen data and compromised health information,

this new virus immediately disrupts day-to-day business functions and the ability to provide high quality health care.

Potential Adverse Outcomes

The primary areas of concerns are the disruption to patient care that occur when a cyber-attack is successful. These attacks can lead to a series of adverse events, including incomplete discharge instructions, missing patient information or orders, potential compromise of Public Health Information (PHI), personal identifiable information (PII), which ultimately could lead to violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, depending on the facility's ability to provide patient care, such as loss of electronic health records or other critical computer based systems, the facility may need to close or temporarily suspend operations.

The Conditions of Participation most impacted for facilities faced with cyber incidents are:

- Governing Body
- Medical Records/ Patient Records
- Nursing Services: due to lack of knowledge of alternate methods such as the medication administration record (MAR), etc.

Recommendations to Providers

CMS recommends that facility leadership review current policies and procedures to ensure adequate plans are in place in the event of an attack. For instance, most IT Directors and policies within facilities require systems to be shut down, and specific timelines to notify appropriate State and Federal agencies and State Health Departments.

Additionally, some providers have shared best practices and mitigation methods, which include retraining of staff to include use of non-electronic methods, such as written discharge instructions, care planning and medical records. Some providers have pre-printed discharge instructions based on common or reoccurring patient care, such as influenza and common cold, and a blank area for additional information which can be hand written by the medical staff. Providers have also encouraged staff to familiarize themselves with the knowledge of the paper medication administration record (MAR) process, and the transmission of laboratory and radiology orders on paper-based requisition forms that are hand delivered to departments for processing. Finally, providers have also taken the initiative to pre-program phone/fax numbers into the fax machine to avoid any delay in the event computer systems are inaccessible.

While the new *Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers* regulation does not specifically address elements of cyber-security, the regulation requires providers and suppliers to have an emergency plan and risk assessment based on an "all-hazards" approach. An all-hazards approach is an integrated approach to emergency preparedness planning that focuses on capacities and capabilities that are critical to preparedness for a full spectrum of emergencies or disasters.

CMS encourages providers to consider cyber-security as an element in the development of their emergency plans, risk assessments, and annual training exercises. While not a requirement, facilities may consider adding cyber security protocols to their policies and procedures. Additionally, given the regulation's requirement for facilities to establish communication plans, which also includes alternate means of communication, the facility could consider addressing within their policies and procedures an element of how to communicate with staff and different departments in the event computers or other means of communication are inaccessible. Finally, facilities may also choose to conduct table-top exercises, with or without assistance from healthcare coalitions or State emergency officials, which are focused on cyber security and how to continue operations in the event of a cyber-attack.

We encourage facility leadership to work with the Chief Nursing Officer (CNO); Risk Manager; Performance Improvement Director; IT Director and Nursing Directors, or anyone the facility deems appropriate in managing cyber-attack mitigation practices. Section 10(b) of Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" requires, "if current regulatory requirements are deemed to be insufficient…agencies identified in sub-section (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions…to mitigate cyber risk." While HHS has concluded that the Department's current regulatory authorities are sufficient, the Department is implementing a number of non-regulatory activities to enhance the cybersecurity of private sector critical infrastructure partners.

Additional Resources

There are several resources for facilities which may assist in overall cybersecurity awareness:

1. The Department of Homeland Security Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities of an organization. See https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CRR_CSET_S508C.pdf
2. Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software (issued Jan. 14, 2005), available at https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm.
3. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks (issued June 13, 2013), available at https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm.
4. Postmarket Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff (December 28, 2016.) Available at https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

We also would encourage facilities to review resources provided by the Office of the Assistant Secretary for Preparedness & Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE) available at https://asprtracie.hhs.gov/.

Contact: Please forward any questions regarding this memorandum to the Survey & Certification Emergency Preparedness mailbox at SCGEmergencyPrep@cms.hhs.gov.

Effective Date: Immediately. This policy should be communicated with all survey and certification staff, their managers and the State/Regional Office training coordinators within 30 days of this memorandum.

/s/
David R. Wright

cc: Survey and Certification Regional Office Management

The contents of this memorandum support activities or actions to improve patient or resident safety and increase quality and reliability of care for better outcomes.