NEW YORK STATE OF OPPORTUNITY. Department of Health

ANDREW M. CUOMO
Governor

HOWARD A. ZUCKER, M.D., J.D.
Acting Commissioner

SALLY DRESLIN, M.S., R.N.
Executive Deputy Commissioner

June 9, 2017

Dear Colleague:

As a Healthcare provider, electronic medical records and medical devices have become an integral component of delivering patient care. Comprehensive cyber security practices are essential to protect these digitally connected systems from disruption and to preserve the capacity of your operations. As recent, highly-visible incidents have demonstrated, exploited system vulnerabilities in one device in one location can lead to the rapid spread of damaging malware across interconnected networks and systems.

While so far, the incidents have not posed an immediate threat to patient safety, these events illustrate that we must remain vigilant in keeping hardware, software, and medical devices protected from emerging threats. To that end, the New York State Department of Health (NYSDOH) and hospital associations are working together and will continue to partner with other federal and state agencies, to develop clear guidelines and processes that foster information sharing and rapid response.

This letter intends to provide initial guidance to NYSDOH regulated, healthcare institutions to minimize the likelihood of a successful breach of IT systems and to remind providers of steps to take once an attempt to penetrate a system has been detected.

Since cyber-attacks and malware outbreaks will continue and do not discriminate in exploiting vulnerable systems, it is critical that healthcare institutions make cybersecurity a priority in risk management. Your information security program must take a comprehensive approach to include vendor requirements and vendor 24/7 contact information, for all forms of digital devices, including medical devices that may not be under the control of your IT department. Resources on the FDA websites are provided in the resource section below for your reference.

In the **short term**, we strongly recommend that you take the following steps:

- Make sure your facility is not at risk to any cyber threats, including WannaCry and its variants. Clear and simple directions for doing this are available from HHS *(see link in attached resource list).*
- Pay special attention to all your devices, including medical instruments, environmental and safety equipment, and automated mechanical systems. If it is controlled by an older version of Windows, check the DHS list of vendors who have released customer recommendations to see if an instrument has been protected *(see link in attached resource list)*. If it is not on the DHS list, contact your vendor to see if it is protected from WannaCry and its variants.
- Review your continuity of operations plan to maintain services during any outages produced by a cyber disruption. We suggest that you confer with your colleagues

in facilities that may have experienced an outage due to a cyber disruption for their best practices. Also, to assist you in defining your mission-essential functions and business processes, we have attached several links *(see link in attached resource list)* that provide guidance on identifying these functions and processes and breaking down their components so that they may be replicated and maintained using a manual, or other workaround process until normal processes are restored.

Finally, to adequately assist, as well as monitor this type of incident and any potential impact to public health, ***please notify your NYSDOH regional office program contacts, or during non-business hours and weekends, the NYSDOH Duty Officer, within 24 hours from the onset of an incident that disrupts normal operations***, and provide regular updates on any operational impacts. Based on the assessment of the risk posed to NYS information systems, you may be barred from accessing any of those systems to avoid further exposure until the situation is remediated to the satisfaction of the relevant NYS Agency. NYSDOH and/or its sister agencies will provide information to providers during an event, as they would in any type of emergency event.

Additionally, providers should be aware of any Federal expectations for identifying the circumstances under which a breach should be detectable, and any Federal reporting responsibility when a breach is detected.

We appreciate your assistance in this matter.

Sincerely,

Sally Dreslin, M.S., R.N.
Executive Deputy Commissioner

Resources:

Wannacry

- **June 2 US HHS notice on WannaCry:** provides mitigating steps, what to do if you are a victim, and pointers to other useful resources including the FDA 24/7 hotline**:** https://asprtracie.hhs.gov/documents/newsfiles/NEWS_06_02_2017_06_15_21.pdf
- **US DHS alert on Indicators of Compromise for WannaCry:** regularly updated, this contains a list of vendors with embedded Windows systems that have customer guidance about WannaCry, as well as links to other resources from DHS, Microsoft, and the FDA: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01
- **US DHS fact sheet on WannaCry,** with simple clear directions about what to do for WannaCry: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware_S508C.pdf

Other HHS cyber resources:

- **CMS Recommendations to Providers Regarding Cyber Security:** https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-17-17.pdf
- **Healthcare Emergency Preparedness Information Gateway:** https://asprtracie.hhs.gov/

FDA Resources

- **General guidance on Cybersecurity:** https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
- **Post Market Management of Cybersecurity in Medical Devices:** https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf
- **FDA Fact Sheet:** https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf

Continuity of Operations (COOP) planning:

- **NYSDOH Continuity for Operations Planning in the Health Care Sector Training** *(October, 2016):* (https://www.urmc.rochester.edu/emergency-preparedness/preparedness-and-response-tools-resources/continuity-of-operations-planning-coop.aspx) This power point course, developed with funding from the CDC Healthcare Preparedness Program provides a concise overview of Continuity of Operations planning.
- ***NYS Department of Homeland Security and Emergency Services (DHSES)*** ***(***http://www.dhses.ny.gov/planning/state/coop.cfm***)*** provides several templates, checklists and continuity resources.
- ***FEMA online training:***
  Continuity of Operations Awareness Course**:**
  https://emilms.fema.gov/IS546.a/index.htm*) and*
  Introduction to Continuity of Operations**:**
  (https://emilms.fema.gov/IS547A/index.htm***)***
- ***FEMA Mission Essential Functions***
  http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-526

- ***FEMA Business Continuity Planning****:* https://www.ready.gov/business/implementation/continuity
- ***FEMA Continuity Circular Two:*** https://www.fema.gov/media-library-data/1386609058826-b084a7230663249ab1d6da4b6472e691/Continuity-Guidance-Circular2.pdf -- This CGC provides guidance and direction to non-Federal Governments (NFGs) for the identification and verification of their essential functions, and the Business Process Analyses and Business Impact Analyses that support and identify the relationships among these essential functions.

ASPR HPP Program:

- https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/hc-coop2-recovery.pdf