HHS Update #5: International Cyber Threat to Healthcare Organizations (CLOSED)

May 17, 2017

HHS will continue to monitor this incident but this will be the final update.

Many thanks to our private/public sector partners throughout this incident. We have done our best to consolidate and answer outstanding questions. ASPR CIP plans to publish a Q&A to the sector in the coming weeks. Below are links to archived updates and information concerning ASPR's After Action submission process.

- Update 1
- Update 2
- Update 3
- Update 4

HHS ASPR's online After Action collection mechanism:

ASPR will be capturing thoughts and comments through an online After Action collection mechanism https://hhscap.hhs.gov. When crafting your After Action comment(s), please consider the following:

- If you have more than one observation to submit, your demographic information will be saved. Please submit one observation at a time.
- All comments, both positive and negative, will be treated in a sensitive manner and all personal information provided will be held confidential by the TELL CAP Working Group Managers.
- Be concise, specific, and honest. Your observation is our only firsthand account of what happened.
- Please include specific names, times, and locations. These are necessary for investigation by the TELL CAP Working Group, but will not be published in final documentation.
- Define all unfamiliar acronyms.
- Recommend specific corrective actions that can be implemented and measured.

Process for victim reporting and indicator sharing:

Note this is not specific to the WannaCry Ransomware and is the process for any cyber attack

If your organization is the victim of a ransomware attack, HHS recommends the following steps:

1. Please contact your FBI Field Office Cyber Task Force (www.fbi.gov/contact-us/field/field-offices) immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cybercrime.
2. Please report cyber incidents to the US-CERT (www.us-cert.gov/ncas) and FBI's Internet Crime Complaint Center (www.ic3.gov).
3. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS' Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC_RM@hhs.gov

FDA's medical device FAQ based on "Daily Sector Call" feedback:

- Medical device manufacturers and healthcare facilities should take steps to ensure appropriate safeguards. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
- Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
- Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
- Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g). For additional FDA guidance, see https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
- Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you suspect that a cybersecurity event has impacted the performance of a medical device or has impacted a hospital network system, we encourage you to file a voluntary report (https://www.fda.gov/Safety/MedWatch/HowToReport/ucm2007306.htm).
- Healthcare personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities (https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm2005737.htm).

Where can I find the most up-to-date information from the U.S. government?

- For overall Cyber Situational Awareness visit the US-CERT National Cyber Awareness System webpage at: https://www.us-cert.gov/ncas
- ASPR CIP maintains the HSIN HPH portal's Cyber Threat Library which contains a "Ransomware" tab with updated information to include indicators and mitigation measures: https://hsin.dhs.gov/ci/hph/Pages/CyberThreat.aspx
- ASPR TRACIE: Healthcare Cybersecurity Best Practices: https://asprtracie.hhs.gov/documents/newsfiles/NEWS_05_13_2017_08_17_11.pdf
- Fact Sheet on the FDA's Role in Medical Device Security: https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf
- CISA Protections for private sector information sharing: https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
- Request an unauthenticated scan of your public IP addresses from DHS. For more information please contact NCATS_INFO@hq.dhs.gov