
# HHS Update #4: International Cyber Threat to Healthcare Organizations (Revised)

May 16, 2017

## If you are the victim of ransomware or have cyber threat indicators to share (**Revised with web addresses**)

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 cyber-crime.
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

## HHS Office of Civil Rights Guidance on HIPAA specific to WannaCry

- As outlined in its guidance available on its website, OCR presumes a breach in the case of ransomware attack. The entity must determine whether such a breach is a reportable breach no later than 60 days after the entity knew or should have known of the breach. A request by law enforcement to hold reports tolls the 60-day reporting deadline. For a copy of the ransomware guidance, please see: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es.
- The ransomware guidance also includes important information about ransomware and how compliance with the HIPAA Security Rule helps entities prepare for ransomware attacks, including with regard to contingency planning. For more guidance on the Rule's requirements, please see https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
- OCR has shared its FAQ on sharing of cyber threat indicators under CISA with federal partners, and it is available on the OCR website. Please see https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/index.html.
- Reporting information to law enforcement, DHS, or other HHS divisions does not constitute inadvertent or intentional reporting to OCR. All reporting of breaches to OCR should be made as required by the HIPAA Breach Notification Rule. Important Note: If the data is not encrypted by the entity to at least NIST specifications when the ransomware attack is deployed, then OCR presumes a breach occurred, due to the ransomware attack. As such, the entity would need to prove, through forensic or other evidence, that the ePHI was encrypted when the attack occurred, and the ransomware containerized (or encrypted again) already-encrypted ePHI. Please see https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

# CISA Protections for private sector information sharing

DHS has provided guidance to non-federal entities sharing threat indicators and defensive measures with federal entities. This document may be useful to private sector legal counsel for interpreting CISA protections. Please visit the below link for details:

https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

# 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
- NCCIC portal for those who have access: https://www.dhs.gov/homeland-security-information-network-hsin

Indicators associated with WannaCry ransomware:

- US-CERT - Alert - TA17-132A - https://www.us-cert.gov/ncas/alerts/TA17-132A
- ICS-CERT - Alert - 17-135-01 - https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01

Healthcare and public health-directed resources:

- 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

# Why connect with your local fusion center?

The federal government leverages the unique skills and capabilities of the National Network of Fusion Centers. With timely, accurate information on potential threats, fusion centers directly contribute to and inform investigations initiated and conducted by federal entities. This National Network is a "force multiplier" in preventing, protecting against, and responding to criminal and terrorist threats.

Find your local fusion center by visiting: https://nfcausa.org/default.aspx/MenuItemID/117/MenuGroup/Public+Home.htm

# FDA's Public Workshop - Cybersecurity of Medical Devices

The U.S. Food and Drug Administration (FDA), in association with National Science Foundation (NSF) and Department of Homeland Security, Science and Technology (DHS, S&T) just announced the upcoming public workshop entitled “Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis.” The purpose of this workshop is to examine opportunities for FDA engagement with new and ongoing research, catalyze collaboration among healthcare and public health stakeholders to identify regulatory science challenges, discuss innovative strategies to address those challenges, and encourage proactive development of analytical tools, processes, and best practices by the stakeholder community to strengthen medical device cybersecurity.

This meeting will be held May 18-19, 2017, from 8:00 am - 5:00 pm at the following location:

FDA White Oak Campus
10903 New Hampshire Avenue
Bldg. 31, Room 1503
Silver Spring, MD, 20993

For further details go to: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm549732.htm

# How to request an unauthenticated scan of your public IP addresses from DHS

The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

- NCATS focuses on increasing the general health and wellness of the cyber perimeter by broadly assessing for all known external vulnerabilities and configuration errors on a persistent basis, enabling proactive mitigation prior to exploitation by malicious third parties to reduce risk.
- Attributable data is not shared or disseminated outside of DHS or beyond the stakeholder; non-attributable data is used to enhance situational awareness.
- NCATS security services are available at no-cost to stakeholders. For more information please contact NCATS_INFO@hq.dhs.gov