COVID-19 Vaccine Operations Security Advisory

February 2021

Attention: COVID-19 Vaccine Providers and Healthcare Partners

This Security Advisory places emphasis on four designated lifeline functions (energy, transportation, water, and communication) to support ongoing security planning at your facility. These functions are intentionally highlighted. If disrupted or loss experienced, it may lead to cascading impacts affecting your COVID-19 operations.

Current Threats: Severe Weather (High Winds, Snow, Ice), Cyber Threats

Energy

Suggestions to limit potential issues in WA for winter weather, high wind events, and wildland fire season this summer.
- All providers are required to have generators
- Questions and steps for Generator Operations:
  ○ When is the last time your organization tested the generator?
  ○ Do you have enough fuel on hand for operation of multiple days?
  ○ When was the last time you requested fuel from your provider?
  ○ Are you on a priority list for fuel delivery from your provider? If not, do you need assistance in getting on the list?

WA had ½ million customers without power during mid-February which caused varying level of impacts. - Have you reached out to your utility provider to ensure you are on the priority emergency restoration list? If you are doing mobile vaccine sites have you been in contact with the utility provider, so they know where these are taking place for awareness on planned outages and emergency restoration if necessary? - Do you have backup plans in place if you do experience a power outage or natural gas outage?
How-to Guides – Generators: - Using Portable/Emergency Generators Safely - Generator Checkup: Maintenance for Safe Service
Transportation
- In February there were a delay of shipments due to winter weather across the nation.   ○ Did you have the appropriate point of contact? Were you able to adjust operations based on this change?

- Road Closures are common due to weather impacts, and rescheduling appointments can occur.
    - How can this process be improved in the future? Were your contingency plans accurate for your facility needs during the recent weather impacts?
- Has your facility experienced any challenges managing the dry ice procedures for holding the vaccines before warming for shot administration?
- Have you experienced any issues ordering dry ice in a timely fashion?

Water/Wastewater

- Did power outages impact your water/wastewater systems during the winter weather?
- Plan and make a list of action items to prepare for inclement weather.
    - Do you have toileting plans for staff and patients in the event of a water outage?
    - Do you have hygiene plans for staff, providers administering shots, and patients in the event of a water outage?
    - Do you have a plan for alternate water source (i.e. bottled water) to meet the consumptive needs (drinking/cooking) of staff?
    - In the event of a long-term water outage, flooding, or contaminated facility, what is your reopening plan.
- Know who your water utility providers are and contact them to let them know you would like to be considered a priority restoration site if there's disruption to service.

Communication / Cyber

Ransomware continues to be a threat to the Healthcare community, below are information to assist you in your cyber security risk posture.
https://us-cert.cisa.gov/ncas/alerts/aa20-302a

- **Health Sector Cybersecurity Coordination Center (HC3) Monthly Cybersecurity Vulnerability Bulletin - PDF**
  In January 2021, a relatively small number of vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public however the ones that were released warrant attention. This includes the Patch Tuesday vulnerabilities – released by several vendors on the second Tuesday of each month – as well as ad-hoc vulnerability announcements including mitigation steps and/or patches as they are developed. Vulnerabilities this month are from Microsoft, Adobe, Intel, SAP, Cisco and Apple. These vulnerabilities should be carefully considered for patching by any healthcare organization with special consideration to each vulnerability criticality category against the risk management posture of the organization.

- **A recent NCSC alert details the massive, ongoing campaign led by Chinese threat actors to steal healthcare, genomic, and valuable data from the US and other countries.**
  NCSC: Chinese Threat Actors Targeting US Healthcare, Genomic Data (healthitsecurity.com)

- **NCIJTF Releases Ransomware Factsheet - Original release date: February 5, 2021**
  The National Cyber Investigative Joint Task Force (NCIJTF) has released a joint-sealed ransomware factsheet to address current ransomware threats and provide information on prevention and mitigation techniques. The Ransomware Factsheet was developed by an interagency group of subject matter experts from more than 15 government agencies to increase awareness of the ransomware threats to police and fire departments; state, local, tribal, and territorial governments; and critical infrastructure entities.

  - To reduce the risk of public and private sector organizations falling victim to common infection vectors like those outlined in the NCIJTF factsheet, CISA launched the Reduce the Risk of Ransomware Campaign in January to provide informational resources to support organizations' cybersecurity and data protection posture against ransomware.
  - CISA encourages users and administrators to review the NCIJTF Ransomware Factsheet and CISA's Ransomware webpage for additional resources to combat ransomware attacks.

- **HHS Cybersecurity Program: Threats in Healthcare Cloud Computing 02/04/21 – PDF**

- **NCSC: CHINA'S COLLECTION OF GENOMIC AND OTHER HEALTHCARE DATA FROM AMERICA: RISKS TO PRIVACY AND U.S. ECONOMIC AND NATIONAL SECURITY**
  Publicly available at https://www.dni.gov/index.php/ncsc-features/2762 (scroll to the bottom of the page to find it, as it's the last item listed). The product references multiple ways in which China has obtained US healthcare data, including via cyber breaches and via research collaboration efforts.

- **Health Sector Cybersecurity Coordination Center (HC3) 2/23/21 – PDF**
  Accellion Compromise Impacts Many Targets Including Healthcare Organizations
  - CISA Releases Joint Cybersecurity Advisory on Exploitation of Accellion File Transfer Appliance
  - AA21-055A: Exploitation of Accellion File Transfer Appliance

Services to Strengthen Cyber Security:

- **"Center For Internet Security Funds No-Cost Service to Help Protect all U.S. Private Hospitals Against Ransomware"**
  https://www.cisecurity.org/press-release/center-for-internet-security-funds-no-cost-service-to-help-protect-all-u-s-private-hospitals-against-ransomware/
  EAST GREENBUSH, N.Y., Feb. 17, 2021 – The Center for Internet Security, Inc. (CIS®) is launching a no-cost ransomware protection service, Malicious Domain Blocking and Reporting (MDBR), for private hospitals in the U.S. today. CIS is fully funding this service for all private hospitals in the U.S. as part of its nonprofit mission to make the connected world a safer place. The service is already available for all public hospitals, health departments, and healthcare organizations through the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC funding for public hospitals is provided by the U.S. Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA).

Emergency Management/Law Enforcement

- If you believe your organization has received counterfeit Personal Protective Equipment (PPE), please contact FBI Seattle.

- Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines.

- All state, local, tribal, and private sector partners are encouraged to report any threats or suspicious activity related to COVID-19 vaccine distribution to local law enforcement agencies, as well as the **Washington State Fusion Center (WSFC)** at **1-877-843-9522**, or **e-mail: intake@wsfc.wa.gov**.

- For information regarding threats to COVID-19 vaccine distribution in Washington go to: **HSIN Washington Infrastructure Protection (WA-IP) > COVID-19 Information**
  - To request a HSIN membership, please send your full name, agency, title/position, and official e-mail to webmaster@wsfc.wa.gov.

- COVID-19 Vaccine Distribution Physical Security Measures (DHS Cybersecurity and Infrastructure Agency)

Additional Federal Resources

- Community Vaccination Centers Playbook (FEMA)

- **Vaccine Prioritization for Critical Infrastructure Workers -** PDF
  The Centers for Disease Control and Prevention (CDC) is the federal lead for recommending how States prioritize vaccine distribution in their jurisdictions.
    - CDC's prioritization guidance has been approved by the Advisory Committee on Immunization Practices (ACIP) and is now available here.
    - You are encouraged to review their guidance and work with your state and local officials on any specific details of how the CDC guidance is implemented in your state or impacting your industry.

- CISA is working with the Department of Health and Human Services, Department of Defense, and other government partners to support the delivery of COVID-19 vaccinations throughout the U.S., including support to the Federal COVID-19 Response.
  COVID-19 Vaccine Rollout | CISA