24-04

STATEMENT OF POLICY
Cybersecurity

Policy

The National Association of County and City Health Officials (NACCHO) strongly urges all local health departments (LHDs), in partnership with state, tribal, territorial, and federal public health agencies, to strengthen their cybersecurity measures; and for the federal government to include LHDs in planning and policy activities related to cyber threats. NACCHO also calls for sufficient federal and state funding support to LHDs and other relevant local stakeholders to engage in multidisciplinary cybersecurity preparedness activities. The increasing magnitude and widespread impact of cybersecurity breaches pose significant threats to human health and safety.

NACCHO has identified cybersecurity resilience as a critical need for LHDs to continue to deliver services and prepare for emergencies in the event of a cyber related disruption, and advocates for the increase of resources to support cybersecurity measures for all LHDs. NACCHO also encourages LHDs to allocate staff and expend resources on developing cybersecurity plans, capabilities, and capacity. However, NACCHO also acknowledges that many LHDs do not have the resources to engage in such activities. NACCHO recommends that federal and state agencies consider the needs of public health agencies as part of strengthening the overall Healthcare and Public Health sector cybersecurity efforts. Additionally, NACCHO recommends the following preparedness and response planning activities:

Readiness

- LHDs are encouraged to align or update current processes on cyber related preparedness with current national strategies, cybersecurity performance goals, and best practices to maintain and safeguard access to public health data and services.
- Building a culture of preparedness for a cyber breach means establishing good cyber hygiene for everyone, regardless of experience. LHDs should practice good cyber hygiene, ranging in activities such as regularly changing passwords, multi-factor authentication, and applying software security patches. These actions play into the role of preventing bad actors from crippling U.S. public health infrastructure.
- LHDs should maintain situational awareness of cybersecurity threats and IT risk assessments that pose a threat to the local public health sector.
- LHDs should consider national strategies and frameworks, such as the National Health Security Strategy (NHSS), National Institute of Standards and Technology (NIST), the

Pandemic and All-Hazards Preparedness & Advancing Innovation Act, and the HPH Cybersecurity Performance Goals, to align their cybersecurity efforts with broader public health preparedness goals.

Partnerships

- Due to the everchanging nature of cybersecurity practices, LHDs should establish or continue collaboration with their local and state IT to stay apprised on updates, new technology, opportunities for funding, and information sharing of the cybersecurity environment.
- LHDs should engage in collective planning and implementation of cybersecurity improvements with their healthcare coalitions (HCC), partners, and stakeholders for increased stabilization of Public Health cybersecurity.
- LHDs are encouraged to collaborate and monitor resources with state Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), and related officials to identify federal support for cybersecurity activities and best practices, including compliance, training, education, and outreach.

Justification

Maintaining a strong cybersecurity infrastructure is essential for the vital work conducted each day by LHDs of all sizes—from rural to urban. They play a critical role in community health and safety, emergency preparedness and response, environmental health, and more. Securing their systems is paramount to maintaining a safe, healthy nation and effective and trustworthy services from LHDs to their communities. Strengthening against bad actors includes ongoing efforts of planning, training, having appropriate hardware, software, and access to expertise to ensure proper configuration and maintenance. It also involves implementing robust protocols for cybersecurity incident response and recovery, and ensuring regular updates are applied to all systems. Collaboration with stakeholders, partners, and national cybersecurity agencies can provide additional layers of protection and intelligence sharing. A proactive, comprehensive approach is essential to safeguard local communities and public health services against cyber threats.

- CYBER THREATS FOR HEALTHCARE AND PUBLIC HEALTH

LHDs play a critical role in lifesaving and life-sustaining activities for their respective community members. Of the threats that can impact the Healthcare and Public Health (HPH) sector, cyber-related disruptions remain on the rise, leading to the need for a more fortified, comprehensive, and strategic approach. Cybersecurity is defined as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[1] As it relates to HPH, cybersecurity refers to the defensive measures and activities that prevent the exploitation or misuse of the cyber infrastructure within HPH sectors.[2] Cyberattacks continue to disrupt critical

infrastructure and put patient privacy and safety at risk. An attack of this nature coinciding with a public health emergency or disaster will further complicate response efforts.

- LHD DATA ON CURRENT STATE OF PREPAREDNESS

Cyber-related disruptions are on the rise, with the HPH sector experiencing a 42% increase in ransomware attacks in 2022 compared to 2021.[3] These disruptions can impact the collection and analysis of epidemiological data, supply chain of medical countermeasures, distribution of emergency supplies, and more. According to NACCHO's 2022 Preparedness Profile, 48% of LHD's feel very concerned about the impact of a cyber-related attack and 26% feel not at all prepared, whereas only 13% feel very prepared.[4]

- WHAT A CYBERSECURITY BREACH MEANS FOR PUBLIC HEALTH

Cyber-related incidents affecting the healthcare and public health sectors have led to extended care disruptions caused by multi-week outages, and to patient diversion to other facilities, alongside the added demand on acute care capabilities, causing "cancelled medical appointments, non-rendered services, and delayed medical procedures."[5] As we take a Public Health focus, a cyber-related disruption could impact case surveillance, immunizations, patient care, family reunification efforts, mass-sheltering, distribution of medical countermeasures (MCM), data sharing on emergency response asset tracking, and other areas within the ever-growing threat landscape. The Health Sector Coordinating Committee (HSCC) Cybersecurity Working Group has developed a strategic plan for 2024-2029. As it applies to public health organizations at the state, local, tribal, and territorial levels, it can be used to "mitigate risk, protect the nation's public health infrastructure and safeguard the interoperable movement of essential data that ensures the public health of entire populations."[6] As stated by the HSCC: Cyber safety is patient safety.

- NATIONAL HEALTH SECURITY STRATEGY (NHSS) & PUBLIC HEALTH EMERGENCY PREPAREDNESS PROGRAM & HOSPITAL PREPAREDNESS PROGRAM

NACCHO's 2022 Preparedness Profile found that only one in three LHDs were aware of the NHSS—a comprehensive strategic approach to coordinating the nation's health security system. The proportion of LHDs aware of this strategy has been declining since 2016.[4] Increasing cybersecurity measures would align with the NHSS Objective 2.4, which is to, "Promote HPH systems and technologies that are protected against and responsive to cybersecurity threats and safeguard patient privacy and medical device security."[7]

The Center for Disease Control and Prevention (CDC) Public Health Emergency Preparedness Program (PHEP) provides operational support to strengthen the security and resilience of the United States through strategic public health preparedness activities. PHEP Capability 6, Information Sharing, emphasizes the need to implement data security and cybersecurity.[8] Data

saves lives, and any risk to accessing and collecting data that can drive decision-making is an inherent threat to the livelihood of our communities.

In conjunction with PHEP activities, the Administration for Preparedness and Response (ASPR) Hospital Preparedness Program (HPP) includes the task of HCCs completing Cybersecurity Assessments for their jurisdictions. The outputs of this assessment will inform other activities, including the Cybersecurity Support Plan and Extended Downtime Support Plan[9]. Public Health sector having this continued funding support from PHEP and HPP programs helps to strengthen the overall HPH sector's resilience to disasters, manmade or natural.

- EXECUTIVE ORDER & NATIONAL SECURITY MEMORANDUM

The 2021 Executive Order 14028, Improving the Nation's Cybersecurity, requires the Federal Government to "improve its efforts to identify, deter, protect against, detect, and respond to [increasingly sophisticated malicious cyber campaigns… and asks the Private Sector to] adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."[10] The National Cybersecurity Strategy lays out the approach to improving the United States cyber defense and securing our digital infrastructure.[11] The plan includes establishing cybersecurity regulations to secure critical infrastructure, using Federal incentives to build security, and holding the stewards of data accountable. As America's healthcare and public health systems continues to undergo a digital transformation, it is critical that Government and industry work together to fulfill the vision of securing both the healthcare and public health systems to protect communities and patients from cyber threats.

National Security Memorandum 22, released in April 2024, empowers the Department of Homeland security to lead the federal government's effort to secure our nation's critical infrastructure alongside CISA. It also "elevates the importance of minimum security and resilience requirements within and across critical infrastructure sectors."[12] Public Health is identified as one of those sectors. NACCHO echoes this need for cybersecurity resilience, supports all local health departments in strengthening their cyber security, and advocates for local health departments to be included in the decision-making, strategy, and funding of efforts to improve cybersecurity in the health sector.

Record of Action

Proposed by the Preparedness Policy Workgroup September 2024

References

1. *Cybersecurity and Infrastructure Security Agency. (2021, February 1). What is cybersecurity? Retrieved April 15, 2024, from https://www.cisa.gov/news-events/news/what-cybersecurity*
2. *Office of the Assistant Secretary for Preparedness and Response. (2014). Healthcare and public health cybersecurity primer: Cybersecurity 101 (HHS Publication). Retrieved October 15, 2014, from http://www.phe.gov/preparedness/planning/ cip/documents/cybersecurity-primer.pdf)*
3. *Healthcare Sector Cybersecurity (hhs.gov)*
4. *National Association for City and County Health Officials (NACCHO). (n.d.). 2022 Preparedness Profile Study. https://www.naccho.org/uploads/downloadable-resources/2022-Preparedness-Profile-Full-Report.pdf*
5. *ASPR. (n.d.). Healthcare and Public Health Cybersecurity. Cybersecurity | Healthcare and Public Health. https://aspr.hhs.gov/cyber/Pages/default.aspx*
6. *Health Industry Cybersecurity – Strategic Plan (2024–2029). (n.d.). https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf*
7. *National Health Security strategy 2023-2026 - ASPR. (n.d.-b). https://aspr.hhs.gov/NHSS/National-Health-Security-Strategy-2023-2026/Documents/nhss-2023-2026-508.pdf*
8. *Centers for Disease Control and Prevention. (2018)Public health emergency preparedness and response capabilities: National standards for state, local, tribal, and territorial public health. U.S. Department of Health and Human Services. https://www.cdc.gov/readiness/media/pdfs/CDC_PreparednesResponseCapabilities_October2018_Final_508.pdf*
9. *Hospital preparedness program (HPP) Cooperative Agreement Guidance. Cooperative Agreement Recipient Reporting Requirements. (n.d.). https://aspr.hhs.gov/HealthCareReadiness/HPP/Pages/CARRR.aspx*
10. *The United States Government. (2021, May 12). Executive order on improving the nation's cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*
11. *National Cybersecurity Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*
12. *The White House. (2024, April 30). Fact sheet: Biden-Harris Administration announces new National Security Memorandum on critical infrastructure. https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/30/fact-sheet-biden-harris-administration-announces-new-national-security-memorandum-on-critical-infrastructure/*