APhA
American Pharmacists Association

AMERICAN PHARMACISTS ASSOCIATION

STATEMENT FOR THE RECORD

BEFORE THE U.S. HOUSE ENERGY AND COMMERCE

OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE

EXAMING THE CHANGE HEALTHCARE CYBERATTACK

MAY 1, 2024

American Pharmacists Association

Chair Giffith, Vice-Chair Lesko, Ranking Member Castor and Members of the Subcommittee:

On behalf of our nation's over 310,000 pharmacists, the American Pharmacists Association (APhA) is pleased to submit the following Statement for the Record to the U.S. House Energy and Commerce Oversight and Investigations Subcommittee Hearing: "Examining the Change Healthcare Cyberattack."

APhA is the largest association of pharmacists in the United States advancing the entire pharmacy profession. APhA represents pharmacists and pharmacy personnel in all practice settings, including community pharmacies, hospitals, long-term care facilities, specialty pharmacies, community health centers, physician offices, ambulatory clinics, managed care organizations, hospice settings, and government facilities. Our members strive to improve medication use, advance patient care, and enhance public health.

The Change Healthcare cyberattack made obvious the deep vulnerabilities of our nation's digital health care infrastructure, resulting in devastating patient care disruption, particularly at community and health system pharmacies across the country. The attack, and even more so the prolonged inability to restore service, severed the lifelines to patient coverage and reimbursement for needed medications. Patients, prescribers, and pharmacies were left in the dark, unsure about medication coverage or patient out of pocket cost. The outage also halted transmission of electronic prescriptions and processing of manufacturer discount cards. Even as reimbursement stopped flowing to pharmacies, pharmacies endeavored to provide appropriate care and medication. However, in many cases, prescription dispensing was inevitably delayed and patient safety was put in jeopardy. This chaos and uncertainty continued for over a month. The full impact of this attack is still unfolding as sensitive and confidential personal health information for hundreds of millions of Americans may have been compromised.

This was a long overdue wake-up call to examine all digital aspects that touch pharmacy operations and data and patient information and care.

The American Pharmacists Association (APhA), representing pharmacists and pharmacy teams in all practice settings, urges policymakers to closely examine the cause, along with patient and business impact, aftermath, responses, penalties, and legal consequences related to the system outages and make the necessary policy changes.

APhA's House of Delegates (HOD), comprised of over 300 delegates from state pharmacy associations, APhA membership, recognized national pharmacy organizations, and ex-officio groups, met during APhA's 2024 Annual Meeting & Exposition in Orlando over March 22–25, 2024, to debate and adopt policy proposals developed throughout the year. The APhA HOD passed the following cybersecurity policy statements.

- APhA advocates for implementation and maintenance of cybersecurity systems, safeguards, and response mechanisms to mitigate risk and minimize harm or disruption for all pharmacies and related parties who manage or access electronic health and business information.
- APhA advocates for all pharmacies and related business entities responsible for electronic health and business information to have cyber liability insurance or an equivalent self-funded plan to protect all relevant parties in the event of a cyberattack and data breach.
- APhA advocates for education providers to facilitate, and pharmacy personnel to seek out, education and training on cybersecurity laws, regulations, and best practices.

APhA recommends the following:

- **Map out the pharmacy ecosystem to identify infrastructure vulnerabilities**
  There are numerous critical infrastructure vulnerabilities in the pharmacy ecosystem that rely on digital technology, where cybersecurity breaches could impact patient safety and continuity of care. These range from exchange of medical product sales and ordering information, claims adjudication, benefit coverage verification, prior authorization, e-prescriptions, reimbursement, Drug Supply Chain Security Act data exchange and verification, risk evaluation and management strategy compliance, prescription drug monitoring programs, controlled substance ordering, management and compliance, and more. There should be public processes, perhaps through the National Academy of Medicine or HHS, to identify these vulnerabilities. Awareness of the critical touch points are important to identify what is needed for prevention, detection, and response related to cybersecurity.

- **Expand accountability for protection of protected health information**
  More and more businesses and providers hold or touch a patient's health information. The Health Insurance Portability and Accountability Act (HIPAA) establishes the framework and requirements for covered entities and certain business associates to safeguard the privacy and security of protected health information (PHI). As health care business models, technology, and threats have advanced, entities that are not subject to HIPAA's requirements may touch, collect, manage, or share electronic patient health information, creating gaps in accountability for the privacy and security of this information. A full analysis of the market participants involved in all corners of health care infrastructure must be completed and policymakers must include these participants as covered entities that must follow HIPAA's requirements in order to expand the reach of accountability and responsibility of PHI.

- **Increase the penalties for breaches and noncompliance**
  Policymakers need to examine the civil money penalties for noncompliance of HIPAA and ensure that they are more appropriately aligned with the scope and breadth of breaches to serve as a better incentive for compliance. Additionally, in the case of breaches such as what happened with Change Healthcare, pharmacies or other impacted entities must not be held financially liable for good faith efforts undertaken during the outage nor subjected to punitive or exploitative actions by pharmacy benefit managers, plans, or impacted patients.

- **Clarify breach notification requirements for downstream covered entities**
  HIPAA requires covered entities and their business associates to provide notification following a breach that compromises the security or privacy of PHI. When PHI that is held by a pharmacy is breached as a result of compromise through another covered entity or business associate, the pharmacy should not be responsible for providing individual breach information. The financial and resource burden on pharmacies could be significant. It should be clear that the entity that was the root source for the breach (e.g., in the latest cyberattack, Change Healthcare) provide the breach notification to all affected parties, and not only the pharmacies or other providers.

- **Require business continuity/backup systems for entities that transmit, hold, or otherwise manage protected health information and heath care business information**
  Continuity of patient care is critical. If care relies on the transmission of data, then those systems must have redundancy and backup plans in place. During the recent Change Healthcare outage, there was no backup or redundancy plans in place to ensure business continuity. Policymakers should require these systems and processes, specifically for any entity that transmits essential health care information related to programs that rely on federal funding, such as Medicare and Medicaid.

- **End vertical integration practices that result in health care market consolidation**
  In the case of Change Healthcare, a serious vulnerability was that industry consolidation and vertical integration resulted in only a few vendors that own nearly all the market share of business for pharmacies and other providers to transact claims. While precise data are not publicly available, several sources estimate that Relay Health and Change Healthcare together control over 95% of the switch aspect in the pharmacy industry. Had an attack simultaneously occurred on Relay Health, the consequences to our system could have been catastrophic.

  Take-it-or-leave-it contracts by entities that dominate the marketplace include provisions that require them to be the sole contractor for certain products and services. This locks

pharmacies in without the ability to switch to a new provider or have a backup plan. Change Healthcare also held sole contracts for many pharmaceutical manufacturer discount cards and compassionate use programs. This meant that not only was the cyberattack disruptive on our system, but it also negatively impacted individuals in our society with health disparities who are particularly vulnerable.

- **Incentivize minimum standards for cybersecurity**
  A balance of voluntary and required minimum standards for enhancing cybersecurity protections by health care entities that touch or hold health care data should be implemented. Incentives are needed to ensure implementation, such as public funding, tax credits, or discounts for publicly available measures and solutions. The government should partner with nonprofit organizations, such as APhA, to create a checklist of measures and efforts to minimize and mitigate exposure to cybersecurity breaches and implement these minimum standards as well as educate the pharmacy community.

  This may include identifying minimum standards and language for model contracts within the pharmacy ecosystem for protection and response of cybersecurity breaches such as:
  - Cyber-insurance coverage
  - Plans for incident response, business continuity, and disaster recovery
  - Vendor management policies
  - Compliance documentation
  - Protocols for authentication and access control, data transmission confidentiality, encryption, vulnerability management, audits, security, training, and use and collection of personal information

- **Establish a federal cyber-insurance program**
  Having adequate cyber-insurance is a best practice as recovery following a cyber security breach can be expensive. The pharmacy community's economic environment is currently in a dire situation and it is difficult for pharmacies to afford to maintain adequate cyber-insurance coverage in the case of breach. Given the importance of strong and reliable public health infrastructure, a federal cyber-insurance program should be established that offers affordable cybersecurity coverage to ensure that pharmacy doors can remain open to provide patient care.

- **Consider and appropriately fund cybersecurity within emergency preparedness and response procedures and practices across the country**
  HHS's Administration for Strategic Preparedness and Response includes cybersecurity within its public health preparedness, response, and recovery portfolio, and works with the

public and private sector on security public health infrastructure. However, cybersecurity needs to be considered a national priority and addressed at the local and state levels by providing appropriate resources and funding to bolster public health cybersecurity preparedness and response plans across the country. This should include tabletop training exercises with health care organizations, including pharmacy, to help the pharmacy community in its preparedness and response.

APhA stands ready to work with policymakers to discuss lessons learned from the Change Healthcare cyberattack, and what's needed to implement these recommendations for prevention, mitigation, emergency preparedness and response, and penalties to ensure this does not happen again. APhA believes that continuity of patient care is paramount and cannot be jeopardized or compromised again. Please contact Doug Huynh, JD, APhA Director of Congressional Affairs, at dhuynh@aphanet.org if you have any additional questions or additional information.