wedi™

Technology Today For A Healthy Tomorrow

May 16, 2024

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Re: Maintaining Data Exchange Following a Cyberattack

Dear Secretary Becerra:

The recent cyberattacks on Change Healthcare and Asension Heath System reveal just how serious the vulnerabilities are throughout the U.S. health care system, and alerted industry leaders and policymakers to the urgent need for enhanced cybersecurity and improved business continuity planning to support redundancies when unplanned outages impact the delivery of health care services. Through engagement with our members, WEDI has identified important data exchange issues that should be addressed by the Department of Health and Human Services (HHS) to mitigate the potential impact of a cyberattack on health care operations. We offer our recommendations and assistance as HHS develops cybersecurity policies and builds outreach programs to educate impacted stakeholders.

WEDI, formed in 1991, is the leading authority on the use of health IT to improve health care information exchange to enhance the quality of care, improve efficiency, and reduce costs of our nation's health care system. WEDI's membership includes a broad coalition of organizations, including health plans, hospitals, other providers, vendors, government agencies, consumers, not-for-profit organizations, and standards development organizations. WEDI was designated in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislation as an advisor to the HHS Secretary.

The Growing Threat of Ransomware Attacks

Ransomware is a type of malware that encrypts the infected device, attached devices or networked drives. Once the malware has encrypted the files, they become unusable without the decryption key. This is when attackers demand a ransom before releasing the devices, and most importantly the data contained in those devices, from their grip. Typically, payment requests take place over non-traditional currencies such as Bitcoin, where any transactions are anonymous and irreversible. Hospitals vulnerable to ransomware may have critical services disrupted that can impact surgeries, life support, and trauma departments. Studies suggest many of these ransoms are paid by health care organizations because they cannot afford the downtime, loss of information, or disruption in critical health care infrastructure. Cyberattacks are usually targeting private information, medical history, and other sensitive patient records. With the rapid adoption of IT in health care infrastructure, many security considerations have been overlooked.

Health care organizations today are greater targets for theft than organizations in other sectors for a few important reasons. The personal health and research information facilities hold are high value commodities to cyber criminals, including nation state actors. Decentralized information systems, where a vendor may use the services of one or more subcontractors, provide for a greater number of potential access points for incursion, putting patient care and privacy at risk. Regardless of their size, health care organizations make attractive cyberattack targets. First, they are financially lucrative targets because of the value of protected health information. Since attackers adjust ransom amounts to the perceived ability of the target to pay, attackers often will hold health information systems hostage until they have extracted maximum ransom payments, utilizing sophisticated tactics to transfer breach threats across criminal enterprises.

Even if no money is paid, the extortion attempt by cyber criminals can still result in extended periods of downtime of the health information system with substantial (and very public) impacts to IT and patient services. The extensive media coverage of cyberattacks on health systems increases the pressure on victims to pay the ransom quickly before it becomes public. Additionally, many health organizations lack the resources to invest in modern, secure IT systems and harden cybersecurity defenses, often relying on outdated or legacy systems that are vulnerable to exploitation. Health organizations can also lack the capacity to respond to and mitigate cyberthreats, which increases the harm caused by cyberattacks as well as the probability of paying ransoms. Another serious consequence is the potential erosion of the patient's trust in the overall health care system.

The recent cyberattacks, while unprecedented, are just the latest example of what has become unfortunately all too commonplace in the health care industry. No health care organization is immune to the threat of cyberattack and countering these threats will require a collaborative effort between the private and private sectors.

WEDI MPA Process

To identify issues and recommendations related to mitigating the impact of a cyberattack on health care data exchange, WEDI leveraged our Member Position Advisory (MPA) process. Our MPA process engaged the WEDI membership through a virtual event with more than 100 members representing health plans, providers, clearinghouses, health IT vendors, Standards Development Organizations, and others. The MPA virtual event provided a venue to discuss various opportunities to reduce the threat of a cyberattack and mitigate the impact of a cyberattack on health care operations.

Recommendations

The following are recommendations we believe will assist the health care industry in preventing cyberattacks and mitigating the impact of a cyberattack on health care data exchange.

- **Create the Office of National Cybersecurity Policy.** The federal government should create a new office called The Office of National Cybersecurity Policy (ONCP); an office led by a "Cyber Policy Czar." While we appreciate that there currently is an Office of the National Cyber Director (ONCD), this office is restricted to performing in an advisory capacity, with no authority to harmonize and coordinate actions taken by other federal agencies before during or after a cyberattack.

  We believe an ONCP could be modelled on the existing Office of National Drug Control Policy (ONDCP) and also be a component of the Executive Office of the President. ONDCP leads and coordinates the nation's drug policy and is responsible for the development and implementation of the National Drug Control Strategy and Budget. ONDCP coordinates across 19 federal agencies and oversees a $41 billion budget as part of a whole-of-government approach to addressing addiction and the overdose epidemic. ONDCP also provides hundreds of millions of dollars to help communities stay healthy and safe through the High Intensity Drug Trafficking Areas Program and the Drug-Free Communities Program.

  The recommended ONCP would not replace any existing agency or usurp any other agency's jurisdiction or function, but rather drive a centralized process of cyber incident reporting, coordinating harmonization efforts across federal agencies stakeholder education (with a focus on under resourced organizations), steer funding for stakeholder cyber preparedness, develop and deploy national contingency planning, and serve as the point agency for industry recovery following a major cyber incident.

- **Conduct Select Audits and Educate the Industry**. HHS, through its Office for Civil Rights (OCR), should conduct proactive, comprehensive select audits of the health care sector. Past OCR audit programs have reviewed policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. Audits present an opportunity to examine mechanisms for compliance, identify best practices, and discover risks and potential vulnerabilities. Specifically, OCR should conduct audits of those covered entities that experienced a cyberattack. Gaining first-hand knowledge of how the attack occurred, systems impacted, contingencies adopted, and post-attacks steps taken could be leveraged to assist other organizations. Through these select audits, OCR can identify best practices that will provide guidance targeted to address compliance challenges.

The aim of the new round of select audits would be to identify cyberattack vulnerabilities of HIPAA covered entities. Rather than conduct these select audits for enforcement purposes, we recommend they be conducted to assess the effectiveness of the current security controls and security gaps (and identify lessons learned) to update controls as appropriate to mitigate risk across the health care infrastructure.

De-identified results from these audits should be leveraged in an educational campaign to better prepare covered entities to address cyber threats. Educational campaigns should be targeted at specific stakeholder groups, sectors that are more frequently targeted by cyber criminals, and those that have limited resources. We encourage HHS to work with industry groups such as WEDI as well as stakeholder-specific professional associations to expand the reach of these important messages.

- **Establish a Voluntary Audit Program**. OCR should be directed to establish a program that would permit covered entities to voluntarily undergo a security audit. This program could be modeled on the Department of Labor’s Occupational Safety and Health Administration’s (OSHA’s) Voluntary Protection Program (VPP) designed to promote effective worksite-based safety and health. In the VPP, management, labor, and OSHA establish cooperative relationships at workplaces that have implemented a comprehensive safety and health management system. The VPP sets performance-based criteria for a managed safety and health system, invites sites to apply, and then assesses applicants against these criteria. OSHA’s verification includes an application review and a rigorous onsite evaluation by a team of OSHA safety and health experts.

  OCR could emulate the approach adopted by OSHA by developing a program that would allow covered entities to have their security policies and procedures reviewed by OCR and any weaknesses detected. Those submitting their policies and procedures for voluntary review should not be subject to enforcement action should any deficiencies be identified during the audit. Rather, the organization should be given sufficient time to correct any issues. This program would be especially important for smaller organizations that do not have the resources required to engage a third-party accreditation/certification vendor.

- **Accredit the Accreditation Programs**. HHS should consider developing minimum standards for third-party accreditation/certification entities. We recognize that there is tremendous value in having independent entities review and accredit/certify that an organization has met or exceeded its proprietary set of security requirements. However, we believe that a minimum set of security, privacy and cybersecurity standards should be mandated to ensure that an accredited or certified organization would be in the best position to avoid a cyberattack or mitigate the effects of a cyberattack.

We also recommend an analysis be undertaken to evaluate the current accreditation/certification bodies (both for profit and not-for-profit organizations) providing services in this space to understand how they are governed, what public and private sector standards are used as "baselines," and how are these standards measured.

Further, the minimum requirements for these accreditation/certification programs should include post attack actions including the implementation of best practices, policies, and procedures related to: (i) identifying and communicating with all trading partners that could potentially be impacted by the cyberattack; (ii) disaster recovery programs to mitigate the impact of a cyberattack on the organization and its trading partners; and (iii) contingency plans to ensure that the organization and its trading partners can continue data exchange following a cyberattack. Given our interconnected health care industry, every effort should be made to expand the coordination of testing programs.

- **Implement Administrative Actions**. As the recent attack on Change Healthcare has shown, data exchange processes can be significantly obstructed during these events. When a health plan, clearinghouse, or supporting vendor is cyberattacked, vital data exchange processes can be impacted. Claims from providers may not be able to be adjudicated, insurance eligibility verifications may not be able to be performed, prior authorizations may not be able to be submitted, electronic prescriptions may not be able to be conveyed, and payments and remittances may not be able to be transmitted.

  These data exchange processes are vital to health care administration and can even affect patient care delivery. Implementing alternative data exchange pathways with the attacked health plan, clearinghouse, or supporting vendor is critical, as is facilitating enrollment in an alternative clearinghouse or vendor, if necessary.

  The industry appreciated the actions taken by HHS following the Change Healthcare cyberattack. Building on these, following a major cyber incident HHS should have in place and be ready to implement some or all of these actions to immediately assist data exchange processes between providers and health plans. These actions could include:

  - Expedite new electronic data interchange (EDI) enrollment. Recent cyberattacks have spotlighted challenges related to enrollment. Providers seeking to move to an alternative vendor for their administrative transactions may encounter significant difficulties changing from one clearinghouse to another for claims processing and other transactions during these outages. It can take weeks or even months for providers to reenroll with another partner, significantly delaying their ability to conduct transactions. Exacerbating these challenges, vendors may also require exclusive contracts. Should that entity be the target of an attack, providers may not have easy access to transfer their data exchange requirements to an alternative vendor.

With this lesson learned from recent cyber incidents, Medicare Administrative Contractors (MACs) should be encouraged to have in place a process for providers to request a new enrollment for the switch. State Medicaid and Children's Health Insurance Program (CHIP) agencies and Medicaid and CHIP managed care plans should also be encouraged to expedite enrollment solutions. Solutions could include the waiving of wet signature requirements on paper enrollment forms, the adoption of bulk enrollment processes to support health systems with numerous clinicians to enroll, and mandated turnaround time for enrollments. HHS should also issue guidance and best practices for non-regulated entities encouraging them to develop expediated enrollment processes.

- Accept Paper Claims. HHS should encourage and assist MACs to be prepared to accept paper claims from providers who need to file them due to the impact of a cyberattack or other incident that impacts their ability to conduct administrative transactions. For some designated period following a cyberattack, MACs should be encouraged to accept paper submissions if a provider needs to file claims in that method.
- Relax or Eliminate Prior Authorization Requirements. HHS should encourage the removal or relaxation of prior authorization, other utilization management, and timely filing requirements should a Medicare Advantage (MA) organization, Part D sponsor, or one of their direct trading partners incur a cyberattack or other incident that impacts their ability to conduct administrative transactions. During a major system outage HHS should encourage all health plans to take similar actions.
- Provide Advance Funding. Should other administrative actions not have the effect of maintaining data exchange processes and continuing claim payments, CMS should explore requiring the MAC or other federally controlled plan directly impacted by the cyberattack to offer accelerated and advance payments (AAPs) to providers most affected by major cyberattack. Other non-impacted plans should be encouraged to offer AAPs should the breadth of the outage warrant such as action. We note as well that the current requirement is for a maximum 30-day payment amount, with repayment in full required 90 days after the AAP is issued. HHS should consider expanding the AAP to a maximum of a 60-day payment amount and a 180-day repayment timeframe.
- Delay or Waive Data Reporting Requirements for Plans and Providers. HHS should adjust the timing requirements (or waive when appropriate) plan and provider data reporting requirements, similar to the flexibility

afforded during natural disasters. Further, HHS should make permanent a "cyberattack" option in the Merit-based Incentive Payment System (MIPS) Extreme and Uncontrollable Circumstances Exception Application to provide relief to providers impacted by a cybersecurity incident.

  - <u>Issue Communication Guidance</u>. One of the challenges the industry faces during and after a cyberattack is the communication between the entity attacked and its trading partners. HHS should issue guidelines for how and when entities hit with a cyberattack should communicate with its trading partners. This guidance should also include recommendations related to the impacted entity's alternative data exchange pathways, options for enrolling with an alternative vendor, any available loan programs or advanced payments, contact information should they wish to reach out to the impacted entity, and any other pertinent information.

    We urge HHS to work with WEDI, the Health Sector Coordinating Council, and other appropriate private sector organizations to assist with disseminating effective, actionable communications across the sector.
  - <u>Explore Opportunities to Increase Cybersecurity Funding.</u> HHS should explore opportunities to leverage existing federal incentive programs and/or create new incentive or grant programs to increase funding for covered entities to invest in cybersecurity. These programs should be targeted at smaller, less resourced entities.

- **Implement an Annual National Health Care Cyber "Fire Drill."** HHS should designate a week as "National Health Care Cyber Fire Drill Week." This would be a designated period (i.e., a week) where HHS (or an ONCP) would lead the health care industry in promoting cyber awareness and action. Health care organizations would be encouraged not only to test internal systems and processes, but also work with their critical trading partners to identify and test systems, alternative data exchange pathways, and contingency plans.

  The Fire Drill should focus on: (i) improving overall cyber hygiene; (ii) internal testing; (iii) employee training; (iv) external testing; (v) contingency planning; (vi) disaster recovery planning; (vii) backup systems/disaster recovery testing; (viii) business continuity testing (trading partner outreach); (ix) awareness of available cybersecurity resources; and (x) other appropriate issues.

As the collective voice of the health care industry on health IT issues, we are pleased to continue our important partnership with HHS and assist in the development and implementation of a national cyber policy that addresses administrative challenges that follow a cyberattack. Close collaboration between government and the private sector is critical if we are to successfully mitigate the potential of harmful impacts associated with these cyberattacks.

We would be happy to meet with the appropriate staff to discuss cybersecurity and the need to maintain data exchange processes during and after a cyberattack. Please contact Charles Stellar, WEDI President and CEO, at 202.329.9700 or cstellar@wedi.org with any questions you may have on the recommendations we have offered in this letter or to discuss collaboration opportunities.

Sincerely,
/s/
Ed Hafner
Chair, Board of Directors

cc: Chiquita Brooks-LaSure, Administrator, Centers for Medicare & Medicaid Services
Micky Tripathi, Ph.D., M.P.P., National Coordinator, Office of the National Coordinator for Health Information Technology
Melanie Fontes Rainer, Director, Office for Civil Rights
WEDI Board of Directors