Artificial Intelligence & Cybersecurity in Health Care
June 20, 2024

As in most industries, health care is feeling the impact of artificial intelligence (AI) as well as dealing with the increasing need for cybersecurity. Both Congress and the Administration are acutely aware of these issues and are attempting to set about dealing with the innovations and issues in a variety of ways. A recent article

Below is an overview of different actions taken on both AI and cybersecurity.

Artificial Intelligence

As with all policies relating to technology, the federal government is very behind and playing catch up now that AI is being integrated into most aspects of health care. A recent article gives a good overview of some actions to review and place rules on AI in the health care industry, click here.

Administration –

- On February 6, 2024, CMS issued a memo to insurers to provide guidance on the use of AI. It states that health insurance companies cannot use AI or algorithms to determine coverage or deny care to members on MA plans. Click here for the memo.
- On January 9, 2024, HHS’ Office of the National Coordinator for Health Information Technology (ONC) published a final rule, “Health Data, Technology, and Interoperability (HTI-1)).” The rule included federal requirements for AI and machine learning-based predictive software in health care. Click here for the final rule and here for the accompanying documents.
  - Additionally, staff from the ONC published a blog in Health Affairs to discuss the objectives of the AI provisions in the final rule, click here.
- On October 30, 2023, the President signed an executive order (EO), “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” The EO established the first set of standards for using artificial intelligence (AI) in healthcare and other industries. The EO seeks to find balance between managing potential risks of AI while encouraging innovation. Click here for the EO, and here for the blog post by Administration officials on the EO.

Congress –

- On February 8, 2024, the Senate Finance Committee held a hearing, “Artificial Intelligence and Health Care: Promise and Pitfalls.” Senators pushed for CMS to take more urgent and aggressive action to prevent health insurance companies from using artificial intelligence to unlawfully deny medical services. Experts who testified before the Committee said just
requiring humans to review recommendations of AI systems is not sufficient to ensure the AI tools are applied fairly and equitably. Click [here](#) to view the hearing and read witness written statements.

- The Algorithmic Accountability Act of 2023 (S.2892/H.R.5628), introduced by Sen. Ron Wyden (D-OR) and Rep. Yvette Clark (D-NY), would require healthcare systems to regularly assess whether the AI tools they develop or select are being used as intended and aren’t perpetuating harmful bias, click [here](#).

- On October 18, 2023, the House Energy and Commerce Committee held a hearing, “Safeguarding Data and Innovation: Setting the Foundation for the use of Artificial Intelligence.” While this hearing was not specifically on the use of AI in health care, the Members and witnesses did discuss the ways that AI could both improve health as well as the ways that it could be abused. General consensus was that there is a great need to establish standards for the usage of AI. Click [here](#) to view the hearing and read the witness statements.

**Cybersecurity**

While for the past few years reports of cyber attacks on health systems have been rampant, this year’s Change Health attack and subsequent massive outage of service has really made policymakers finally become more alert to the issue. There have been a series of hearings on Capitol Hill and initiatives by the Administration looking into what happened at Change Health and looking into how to prevent such an attack in the future.

**Administration –**

- On May 30, 2024, HHS' Office of Civil Rights published an update to the frequently asked questions webpage stating that hospitals and clinics can require that UnitedHealth Group Inc. notify patients if their data was compromised in a massive February cyberattack on the insurer's payments unit, click [here](#).
- On April 4, 2024, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a proposed rule implementing cyber incident and ransom payment reporting requirements, intended to help the agency prevent cyberattacks and deploy assistance to victims, click [here](#).
- On May 20, 2024, the Advanced Research Projects Agency for Health (ARPA-H) introduced the Universal Patching and Remediation for Autonomous Defense (UPGRADE) program, an initiative aimed at fortifying cybersecurity defenses within healthcare facilities, click [here](#).
- On March 25, 2024, HHS put out a guide to health plan resources for health care providers impacted by the Change cyberattack, including health plan contact information, click [here](#).
- The President's budget has a provision for an $800 million set aside for hospitals to help them meet minimum cybersecurity standards. The details are on page 83 of the White House budget proposal summery, click [here](#).
- In their 2023 Internet Crime Report, the FBI unveiled the escalating dangers within today's cyber landscape, as an assortment of malicious actors continues to wield sophisticated tools to perpetrate large-scale fraud, ransom schemes, and jeopardize national security, click [here](#).
- The Administration's National Cybersecurity Strategy looks to emphasize the need for robust cybersecurity measures, including regulatory frameworks and Federal incentives, to fortify critical infrastructure. Click [here](#) to read HHS' proposed framework to bolster cybersecurity.
HHS' Administration for Strategic Preparedness and Response published voluntary cybersecurity performance goals tailored for healthcare organizations. Hosted on the new gateway website, the goals are broken into two categories, "Essential Goals" and "Enhanced Goals," that reflect cybersecurity frameworks, best practices, and strategies developed by the healthcare industry. The voluntary goals lay out the prioritization for layers of protection across various points of weakness for health care providers. To view the gateway website, click here, and for the goals document, click here.

Congress –
- On June 5, 2024, Senate Finance Committee Chairman, Ron Wyden (D-OR) urged HHS to require health care companies to improve their cybersecurity practices, and to protect against cyberattacks. HHS' current approach is to offer best practices and allow health care companies to "self-regulate" cybersecurity practices, click here.
- On May 30, 2024, Senate Finance Committee Chairman, Ron Wyden (D-OR) sent a letter to Federal Trade Commission and U.S. Securities and Exchange Commission telling the agencies to hold UnitedHealth Group accountable for negligent cybersecurity practices that led to the ransomware attack on Change Healthcare, click here.
- On April 16, 2024, the House Energy and Commerce Committee held a hearing, “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack.” While UnitedHealth (owner of Change Healthcare) did not send a witness, witnesses that were present, including AHA, cybersecurity experts, and a physician in private practice, described the massive disruption to health care provider. Members – both Republicans and Democrats – questioned how consolidation in the insurance and health technology industries is impacting provider abilities. Click here to view the hearing and read written statements.
- On March 22, 2024, Sen. Mark Warner introduced legislation - the Health Care Cybersecurity Improvement Act of 2024 - that would allow for advance and accelerated payments to health care providers in the event of a cyber incident, as long as they and their vendors meet minimum cybersecurity standards, click here.