Health Care Industry Cybersecurity Task Force Report Identifies Imperatives for Reform

MAY 8, 2017

Several media organizations this week published a pre-release copy of the report of the Health Care Industry Cybersecurity Task Force established pursuant to the Cybersecurity Act of 2015. The report, written by a 21-member public-private group selected by the Secretary of Health and Human Services (HHS), identifies six “imperatives” for improving cybersecurity in the health care sector, with groups of concrete recommendations for action under each imperative.

Describing cybersecurity as “a key public health concern that needs immediate and aggressive attention,” the report describes a number of factors contributing to the critical state of health care cybersecurity, including the rapid move by many health care providers to electronic health record (EHR) systems—a transition incentivized by government subsidies—and the absence of a central regulatory authority with responsibility for cybersecurity across the health care industry. The six imperatives and some of the most noteworthy recommended action items are:

- **Define and streamline leadership, governance, and expectations for health care industry cybersecurity**. The report recommends:
  - establishment of a “cybersecurity leader” role at HHS to help guide cybersecurity efforts in the health care sector;
  - creation of a “health care-specific” version of the Cybersecurity Framework developed by the National Institute of Standards and Technology;
  - harmonization of cybersecurity laws and regulations affecting health care organizations;
  - consideration of amendments to the Physician Self-Referral Law (the “Stark Law”) and the Anti-Kickback Statute to permit larger health care entities to provide smaller partners with cybersecurity advice, technology, and expertise; and
  - adoption by regulators of a more lenient approach to security breaches caused by “mistakes and slips,” to encourage the sharing of information about breaches without fear of regulatory sanctions.
- **Increase the security and resilience of medical devices and health IT**. The report recommends:

    - cooperation by vendors and health care providers to inventory and secure legacy systems;
    - adoption of "strong authentication to improve identity and access management" and "strategic and architectural approaches to reduce the attack surface" for both medical devices and EHR systems; and
    - creation of a Medical Computer Emergency Readiness Team that could be called upon to "coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures."
- **Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities**. The report recommends:
    - hiring by health care organizations of qualified cybersecurity personnel and establishment of leadership positions within their organizations with responsibility for cybersecurity; and
    - development of secure and cost-efficient storage solutions for smaller organizations to handle EHRs.
- **Increase health care industry readiness through improved cybersecurity awareness and education**. The report recommends:
    - education by health care organizations of their leadership about cybersecurity risks;
    - creation of a "conformity assessment model" that could be used to evaluate new technology and software for cybersecurity issues; and
    - development of more tools to enable consumers to manage and assess cybersecurity protections.
- **Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure**. The report recommends:
    - additional academic research on methods for protecting health care data sets; and
    - creation of guidance for industry and academia on how to create an "economic impact analysis" describing the "cybersecurity risk for health care research and development."
- **Improve information-sharing concerning industry threats, weaknesses, and mitigations**. The report recommends:
    - packaging cyber-risk information in a manner that allows persons with part-time cybersecurity responsibilities to act on it, with a focus on the cybersecurity needs of small and medium-sized health care providers; and
    - greater information-sharing "across the health care industry."

The Task Force's report notes that it found the "engagement with other federal and private sector partners" to be very helpful, and suggests "the establishment of an ongoing public-private forum" to "enhance cybersecurity discussions and protections."

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

✉ benjamin.powell@wilmerhale.com

☎ +1 202 663 6770

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP