DORSEY
DORSEY+WHITNEY LLP

Cybersecurity Task Force Issues Report on Improving Cybersecurity in the Health Care Industry

June 19, 2017 – Dorsey Health Law
by Ross C. D'Emanuele

The *Cybersecurity Act of 2015* established the Health Care Industry Cybersecurity Task Force to respond to severe cyber-attacks within the rapidly-expanding information technology ("IT") aspect of health care. Section 405(c) of the Act required the Task Force to research and develop a report summarizing the vulnerabilities in health care IT. On June 2nd, 2017, the Task Force released its *Report on Improving Cybersecurity in the Health Care Industry*. The Report is sobering, and finds that health care cybersecurity is in critical condition. The Report outlines six recommendations to improve cybersecurity in the health care industry:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, risks, and mitigations.

These six recommendations recognize the need to assess cybersecurity at the industry level in order to better protect patient care and security. To use a cliché, health care cybersecurity will only be as strong as the weakest link in the industry. However, not every health care entity has similar resources. So, while the recommendations call for improvements and updates to guidance, regulations, and laws that affect health care cybersecurity, they do so in a way that recognizes the need for flexibility in the health care industry. For example, the first recommendation calls federal legislation "confusing" and "conflicting" and asks for a unified regulatory framework that untangles the current mess. In addition, the recommendations illustrate that the growing sophistication of health care IT demands a broader cybersecurity approach than previously required. The cybersecurity concern no longer rests with only protected health information at the

Related People

- Ross C. D'Emanuele

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

provider level. Now, cybersecurity needs to branch out and include, for example, medical device developers.

Improving patient care is clearly a central goal, and the Report speaks to that objective by highlighting problem areas with a direct connection to patient care outcomes. The Report also recognizes that the health care industry is a mosaic of large systems, private practices, payers, and developers where a one-size-fits-all approach is not conducive to progress. As such, this Report may trigger a cybersecurity-themed review of various regulatory areas that takes into account both patient care needs and variations in health care entity resources.

Summer Associate Randall Hanson provided substantial assistance with the drafting of this blog post.