Drinker Biddle

Client Alert

June 8, 2017

Disrupting the Health Care Cybersecurity Model (or Lack Thereof): Health Care Industry Cybersecurity Task Force Calls Out Regulatory Barriers

By Emily J. Maus, Sumaya M. Noush and Krissa L. Webb

The Health Care Industry Cybersecurity Task Force ("the Task Force") released the Report on Improving Cybersecurity in the Health Care Industry on June 2, 2017. This Alert follows a previous Drinker Biddle publication that identified the six high-level imperatives around which the Task Force organized its recommendations and action items. Below, we discuss three themes of the report and their potential impact on the existing health care regulatory environment: (1) consolidation of development and oversight of a comprehensive health care security framework; (2) creation of government and private incentives to migrate vulnerable health care providers to more secure environments; and (3) development of new exemptions to fraud and abuse laws to foster collaboration and permit shared resources among health care providers.

HHS and a Comprehensive Health Care Security Framework

A central discussion of the report is the multiplicity of actors involved in the cybersecurity infrastructure within the health care sector, and how they might be aligned around a single unifying strategy. The report notes that because agencies have specific charges, oversight, existing regulatory structures and funding complications, no single agency currently has the capability to address all cybersecurity issues in health care. The report therefore notes the need to develop a unified cybersecurity framework that functions at an interagency level.

To best streamline leadership, governance and expectations for health care cybersecurity, the Task Force recommends the creation of a cybersecurity leadership role within HHS in order to align the agency's internal efforts. The recommendation rests on the scope of HHS' existing authority over health care cybersecurity matters, which the Task Force suggests could be functionally pulled together under a unifying framework if coordinated by a single person and point of entry looking comprehensively at cyber risks.[1] The Task Force then suggests that HHS take the lead in creating a consistent, consensus-based, health care-specific Cybersecurity Framework to align the efforts of private, federal and state actors in advancing health care cybersecurity. The report suggests this framework could build on the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule to promote a single lexicon for health care, as well as standards, guidelines and best practices.[2]

The Task Force also suggests that the initial work by federal regulatory agencies should prioritize harmonizing existing and future laws and regulations that affect health care industry cybersecurity. Currently, a broad patchwork of state and federal laws around data breach, data disposal and data security create significant compliance burdens for health care providers. When considering an overarching cybersecurity framework, regulatory agencies should endeavor to ensure consistency among various federal and state cybersecurity regulations. This would enable health care providers to focus on deploying their resources appropriately between securing patient information and the quality, safety and accessibility of patient care, instead of focusing on statutory and regulatory inconsistencies. The report recommends HHS coordinate with state and federal partners to harmonize regulations, recommend statutory changes to Congress, and publish guidance developed around the structure of the NIST Cybersecurity Framework.

Government and Private Incentives to Migrate Vulnerable Health Care Providers to More Secure Environments

The report also defines some mechanisms to help prioritize cybersecurity in the health care industry, paying particularly close attention to the heightened cybersecurity vulnerabilities of small and medium-sized health care providers, non-profit providers, clinicians and rural hospitals.

1 The Task Force does not specifically address whether this leadership role would involve re-evaluation of the existing health privacy and security framework of HIPAA/HITECH. However, should this report encourage Congress to pursue the development of a more unified cybersecurity framework, existing laws and regulations may be impacted.

2 We note that a current crosswalk exists between HIPAA and the NIST standards, mapping administrative, physical and technical safeguards in HIPAA to a relevant NIST Cybersecurity Framework subcategory providing detailed assessments of cybersecurity risks.

According to the report, tight profit margins and limited resources increase small and medium-sized health care providers' cybersecurity vulnerabilities and hinder technological progress. The Task Force recommends that these providers, in part, look beyond the confines of current legacy electronic health record (EHR) systems and technological infrastructure and shift to a model of *transferring* health care information to more secure environments, such as secure cloud computing environments. These secure environments offer a variety of controls and technologies to resource-constrained providers that allow them to more fully focus their clinical resources on supporting patients instead of maintaining on-premises infrastructures. The report acknowledges that these relationships would still be regulated by federal and state health care privacy and security laws, such as HIPAA.

To facilitate disrupting the current cybersecurity models, or lack thereof, the Task Force suggests eliciting participation and cooperation from government and private payors. The Task Force recommends that the federal government and private payors evaluate incentive options, such as grants and tax incentives, to help develop secure options for small and medium-sized health care providers and to encourage health care providers to migrate to more secure environments. In doing so, the report introduces a heightened level of responsibility across all actors, not just health care providers, to meet the urgent challenges that cybersecurity issues create.[3]

Development of Fraud and Abuse Exemptions to Foster Collaboration and Permit Shared Resources

Finally, the report encourages Congress to consider adjustments to fraud and abuse laws to reduce health care providers' risk of potential penalty in any cybersecurity alignment that involves shared resources or exchanges of value.

As the report repeatedly identifies, health care providers do not have the resources necessary for quick implementation of new technology and cybersecurity practices. Technology is expensive and changes in technology and its utilization require time and energy – two vital resources which health care providers have a duty to devote to patient care. Accordingly, providers need meaningful financial and business incentives to address the overwhelming costs of technical advancement and create space to prioritize technological development and benefit from economies of scale. This means that providers will also need protection from federal laws and regulations that antagonize exchanges of value and certain brands of industry alignment. Accordingly, the Task Force encourages Congress to consider adjustments to current fraud and abuse laws, including the Stark Law and the Anti-Kickback Statute, to acknowledge the need to create space for alignment and financial support between large and small industry players.

By way of example, the report points to regulatory safe harbors and exceptions that have previously been developed in order to facilitate the subsidy of EHR technology between large and small health care providers. These exceptions have successfully advanced EHR adoption throughout the industry, and provide a useful blueprint for similar exceptions that would permit subsidy or donation of more advanced cybersecurity technology and resources. Though the report's recommendations here are expressly directed at Congress, it is reasonable to infer that regulatory authorities are also considering the creation of fraud and abuse exceptions or exemptions within their own jurisdictions. Immunizing certain actions or relationships would target the very real economic barriers to cybersecurity alignment that providers currently face and facilitate the transition into meaningfully reducing cybersecurity threats.

Conclusion

Although health care cybersecurity is in critical condition and there is no silver-bullet solution, the imperatives described in the report are reminders that the health care industry needs to break through current cost, operational and regulatory barriers, and enter into a new age of health care industry infrastructure. The report recommends that the government lead an aggressive and coordinated revolution of reforms to make health care information more secure and health care systems less vulnerable to attack. Stay tuned for future articles on the impact of this report on the health care industry.

3 This report builds alongside other architecture, such as the Modernizing Government Technology Act of 2017 and the Creating Opportunities Now for Necessary and Effective Care Technologies (CONNECT) for Health Act of 2017, to help incentivize the creation of a safer, more modernized information technology and cybersecurity ecosystem.

Health Care Team

Primary Contacts

Emily J. Maus
Associate
Washington, D.C.
(202) 230-5616
emily.maus@dbr.com

Sumaya M. Noush
Associate
Chicago
(312) 569-1268
sumaya.noush@dbr.com

Krissa L. Webb
Associate
Washington, D.C.
(202) 230-5615
krissa.webb@dbr.com

DrinkerBiddle®
www.drinkerbiddle.com
CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON