GIBSON DUNN

January 14, 2019

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES ISSUES NEW GUIDANCE ON VOLUNTARY CYBERSECURITY PRACTICES FOR HEALTH CARE INDUSTRY

To Our Clients and Friends:

On December 28, 2018, a Task Group that includes U.S. Department of Health and Human Services ("HHS") personnel and private-sector health care industry leaders published new guidance for health care organizations on cybersecurity best practices.[1] The guidance—*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*—is voluntary and creates no legal obligations. It is targeted to health care providers, payors, pharmaceutical companies, and medical device manufacturers.

This publication is among the most comprehensive and detailed guidance now available to the health care industry on cybersecurity. While voluntary, the prescriptive advice and scalable tools in the new guidance may be a valuable resource for legal, compliance, IT, and information security professionals at health care organizations. Organizations that follow this guidance may decrease the likelihood that they will suffer a costly data breach, and in the event of a breach may be able to point to compliance with the guidance to show that they have implemented reasonable cybersecurity practices, thereby helping to defend against private lawsuits or government enforcement actions.

This alert briefly describes the background and key takeaways from the guidance. Gibson Dunn is available to answer any questions you may have about how this guidance applies to your organization, as well as any other topics related to cybersecurity or privacy in the health care industry.

Background

The health care industry is a primary target for attacks by cyber-criminals. The threat is especially critical because by at least one measure the average cost of a data breach in the health sector is $408 per record, almost *double* that of the next highest industry.[2] In recent years, moreover, HHS's Office for Civil Rights ("OCR")—the office charged with enforcing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")—has demonstrated an increasing willingness to bring enforcement actions against even reputable and respected organizations that have suffered a data breach.[3]

The new guidance comes against this backdrop and as the result of the Cybersecurity Act of 2015, which required HHS to issue guidance through a "trusted platform and tighter partnership between the United States government and the private sector."[4] Under Section 405(d) of the Act, industry and government leaders formed a Task Group in May 2017 to create a set of "voluntary, consensus-based principles and

practices to ensure cybersecurity in the Health Care and Public Health (HPH) sector."[5] This guidance is the result of 18 months of work by the Task Group.

The Guidance

Recognizing that it would be impossible to address every cybersecurity challenge in a single publication, the Task Group focused on five prevalent cybersecurity threats: 1) e-mail phishing attacks, 2) ransomware attacks, 3) loss or theft of equipment or data, 4) insider, accidental or intentional data loss, and 5) attacks against connected medical devices that may affect patient safety.[6] For each of the five high risk cybersecurity threats, the guidance describes the risk, lists specific vulnerabilities and the potential effects of these vulnerabilities, and offers a list of "practices to consider" to help minimize the threat.

The Task Group then identified a set of voluntary best practices and organized them into ten categories:

1. E-mail Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Information regarding each of these practice categories is detailed in two supplementary technical volumes—one addressing the needs of small organizations and the other addressing the requirements of medium and large organizations—as well as a supplemental volume of additional resources and templates. The guidance also provides a toolkit for determining and prioritizing the cybersecurity practices that would be most effective, which can be used to assist organizations in conducting a cybersecurity risk assessment.[7]

The specific practices identified in the guidance are not intended to replace existing regulatory requirements or frameworks (such as the HIPAA Security Rule or the NIST Cybersecurity Framework). Instead, they are intended to be a supplemental resource for health care organizations, with the goal of "rais[ing] the cybersecurity floor across the health care industry."[8] Specific application and

resource allocation will be up to each organization, and the guidance recognizes that each organization will need to tailor cybersecurity practices to its specific size, complexity, and type. The guidance provides a chart to assist in determining these categorizations.[9] Importantly, the guidance does not authorize any causes of action or grounds for regulatory enforcement.

Conclusion

Because of the long shadow of HIPAA, the health care industry has long been among the most heavily-regulated industries when it comes to cybersecurity practices. This new guidance offers an additional tool that health care organizations can use to gauge the adequacy of their systems and their preparedness for a cyber attack. Given that HHS OCR is simultaneously seeking comments on how it might update HIPAA's requirements,[10] and the explosion of enforcement activity and lawsuits related to cybersecurity and privacy more generally, health care organizations would be well-served to evaluate this guidance and refine or enhance their plans to address cybersecurity issues that regulators and plaintiffs are likely to examine increasingly in the years to come.

---

[1] Healthcare & Public Health Sector Coordinating Councils, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (Dec. 28, 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.

[2] *Id.* at 9.

[3] *See, e.g.*, Press Release, Department of Health and Human Services, *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History* (Oct. 15, 2018), https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html, Press Release, Department of Health and Human Services, *Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules* (Feb. 1, 2018), available at https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.

[4] *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, at 4.

[5] *Id.*

[6] *Id*. at 6.

[7] *Id.* at 26.

[8] *Id*.

[9] *Id.* at 11.

[10] *See* Request for Information on Modifying HIPAA Rules to Improve Coordinate Care, 83 Fed. Reg. 64,302 (Dec. 14, 2018).

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, or the following authors:

Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Reid Rector - Denver (+1 303-298-5923, rrector@gibsondunn.com)
Josiah J. Clarke - Denver (+1 303-298-5708, jclarke@gibsondunn.com)

Please also feel free to contact the following practice group leaders:

Alexander H. Southwell - Chair, Privacy, Cybersecurity and Consumer Protection Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Daniel J. Thomasch - Co-Chair, Life Sciences Practice, New York (+1 212-351-3800, dthomasch@gibsondunn.com)
Tracey B. Davies - Co-Chair, Life Sciences Practice, Dallas (+1 214-698-3335, tdavies@gibsondunn.com)
Ryan A. Murr - Co-Chair, Life Sciences Practice, San Francisco (+1 415-393-8373, rmurr@gibsondunn.com)
Stephen C. Payne - Chair, FDA and Health Care Practice, Washington, D.C. (+1 202-887-3693, spayne@gibsondunn.com)