Bond

INFORMATION MEMO
HEALTH CARE
CYBERSECURITY AND DATA PRIVACY

FEBRUARY 1, 2019

U.S. Department of Health and Human Services Issues Cybersecurity Guidance For Health Care Providers

The U.S. Department of Health and Human Services ("HHS"), in conjunction with the Health Sector Coordinating Council has released cybersecurity guidelines (the "Guidelines") to assist health care providers and inform best practices. Entitled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," the Guidelines are divided into sections for small, medium and large health care providers, recognizing that security programs will vary with the size, resources and information technology capacity of organizations. This approach is a core premise of the HIPAA Security Rule.

Developed collaboratively between HHS and industry cybersecurity leaders, the Guidelines are consensus-based and set forth concrete recommendations. In the face of the extraordinary degree of data exchange occurring in the health care arena to accomplish population health management and value-based payment, the Guidelines are a timely and highly useful resource.

The report that accompanied the Guidelines ("Report") highlights the increase in the number and sophistication of cybersecurity attacks in 2016 and 2017, emphasizing that not only large but small organizations are at risk because hackers assume that smaller entities are more vulnerable to attack. The Report provides some sobering data, noting that the average data breach cost per health care record is $408, with $2.2 million as the average cost of a data breach for health care organizations.

The Guidelines are organized to address the five cybersecurity events identified as the highest threats to health care organizations:

- E-mail phishing attacks,
- Ransomware attacks,
- Loss or theft of equipment or data,
- Data loss, and
- Attacks against connected medical devices with patient safety ramifications.

The introduction to the Guidelines discusses current threats facing the health care sector. The first and second volumes of the Guidelines discuss cybersecurity practices for small, medium and large health care providers. The Guidelines are organized into 10 areas of cybersecurity practices targeted to combat the threats listed above:

- E-mail protection systems
- Access management
- Asset management
- Vulnerability management
- Medical device security
- Endpoint protection systems
- Data protection and loss prevention
- Network management
- Incident response
- Cybersecurity policies.

For each practice, the Guidelines set forth specific recommendations organized by size of provider, covering areas such as authorization procedures, network configuration, multifactor authentication, data classification, and workforce training. The recommended practices address key elements of the HIPAA Security Rule and align with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, the leading national standard for cybersecurity.

The last volume of the Guidelines contains an outline for prioritizing and implementing the practices, along with policy templates and links to other resources. Overall, the Guidelines are a valuable resource for health care providers in addressing cybersecurity threats. It should be noted that while the Guidelines are voluntary, they may set an industry standard that could be used in litigation or other contexts.

If you have any questions about the Guidelines, contact Tracy E. Miller, Deputy Chair of the Health Care Practice and Co-Chair of the Cybersecurity and Data Privacy Practice, Logan Geen, or the attorney in the Firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Bond has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, www.bsk.com. • Attorney Advertising • © 2019 Bond, Schoeneck & King PLLC

CONNECT WITH US ON LINKEDIN: SEARCH FOR BOND, SCHOENECK & KING, PLLC
FOLLOW US ON TWITTER: SEARCH FOR BONDLAWFIRM