Business Advocate®
presented by McDonald Hopkins

Guidance Recommends Health Care Cybersecurity Best Practices

RICK HINDMAND, EMILY JOHNSON | HEALTHCARE PRESCRIPTIONS | JAN 09, 2019

As 2018 was winding down, the Department of Health and Human Services (HHS) on December 28 released Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, a four volume publication identifying the top five health care cybersecurity threats and setting forth voluntary cybersecurity best practices for a wide variety of health care organizations (the "Cybersecurity Guidance").

THE CYBERSECURITY GUIDANCE

The Cybersecurity Guidance was developed by a public-private task group of over 150 cybersecurity and health care experts that HHS convened under the Cybersecurity Act of 2015 to raise cybersecurity awareness and recommend voluntary, consensus-based practices that health care organizations of all types and sizes can use to cost-effectively enhance cybersecurity. The main document cites statistics and examples to illustrate the prevalence and high cost of data breaches. In particular:

- The average cost of a health care data breach is $2.2 million
- The data breach cost per record for health care increased to $408 in 2018 and is the highest of any industry
- On average, health care organizations spent smaller portions of their IT budgets on cybersecurity than non-health care organizations.
- 60 percent of small businesses go out of business within 6 moths of a cyber attack
- 80 percent of physicians have experienced some form of cybersecurity attack.

The task group recognized that it would be impractical to address all cybersecurity challenges, and so identified the following as the top five cybersecurity threats to the health care industry:

- E-mail phishing attacks
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that may affect patient safety

To reduce risks from these threats, the task group recommends the following as the ten most effective practices:

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

The Cybersecurity Guidance divides each of the best practices identified above by organization size (small, medium or large), acknowledging that larger organizations are generally more complex. Large organizations are encouraged to review the sub-practices for both medium and large organizations, and medium-sized organizations are encouraged to consider the large organization sub-practices that apply to their needs. The main document includes a table describing “best fit” characteristics for determining whether a particular organization should follow the sub-practices for a small, medium or large organization.

The recommended practices are aligned with the National Institute of Standards and Technology framework, which is designed to manage cyber threats through the concurrent cybersecurity life cycle functions of identify, protect, detect, respond and recover.

IMPLICATIONS

The Cybersecurity Guidance is another reminder in a long line of reminders from HHS of the need to implement reasonable cybersecurity safeguards, and follows close on the heels of the September 2018 release by the Cybersecurity Unit of the Department of Justice of its updated Best Practices for Victim Response and Reporting of Cyber Incidents, which outlines recommended steps to prepare for and respond to cyber incidents**.**

The Cybersecurity Guidance will benefit a wide range of health care organizations, as well as patients and other stakeholders, by raising awareness of cybersecurity risks and sharing practical steps to enhance cybersecurity. The stated purpose is not to create a new framework or regulatory requirement, but to “help raise the cybersecurity floor across the health care industry regarding our defensive and responsive cybersecurity practices."

Plaintiffs' attorneys for data breach victims are likely to equate the recommended practices with the cybersecurity standard of care and point to the Cybersecurity Guidance in support of holding an organization liable for any breaches that could have been prevented by the recommended practices. Regulators, such as the HHS Office for Civil Rights (OCR), the Food and Drug Administration (FDA) and state attorneys general, may also look to the recommended practices in determining whether reasonable safeguards have been implemented and in establishing future standards.

ACTION PLAN

On the date the Cybersecurity Guidance was released, HHS Acting Chief Information Officer Janet Vogel said "cybersecurity is everyone's responsibility. It is the responsibility of every organization working in healthcare and public health." The ever-evolving nature of cybersecurity proves that compliance must be ongoing and continuous to minimize risk and protect patient privacy.

The recommended practices are intended as a starting point for basic cybersecurity practices. Each health care organization should review the recommended practices for its size, compare its existing practices to the recommended practices, and determine how to revise its policies and procedures to more effectively address cybersecurity concerns.

The Cybersecurity Guidance includes an appendix setting forth an assessment process involving the following five steps to select and prioritize the threats and best practices of most importance to a particular health care organization:

1. Enumerate and prioritize the threats.
2. Review the practices that mitigate each threat.
3. Determine gaps between the recommended sub-practices for each threat and the organization's existing safeguards.
4. Identify and implement cost-effective improvement opportunities.
5. After applying steps 1-4 for the top priority threat, repeat the steps for the next priority threat, and so on for lower priority threats.

The best practices are meant to be considered as only part of an organization's overall cybersecurity program, and are intended to be recommendations and not the only solution. Additional steps of particular importance for health care organizations include:

- Conduct and regularly update enterprise-wide risk analyses (sometimes referred to as "risk assessments").
- Update privacy, security and breach notification policies and procedures.
- Implement an incident response plan and incident response team and regularly and periodically test both.
- Identify all business associate relationships, vet vendors and suppliers who access patient or other confidential information, and ensure that appropriate business associate agreements are in place (**"Who is a HIPAA Business Associate"**).
- Conduct ongoing privacy and security training.
- Consider cybersecurity and related insurance coverage to minimize the potential expenses of a breach.
- Don't forget paper records and the possibility of old fashioned breaches.
- Monitor additional threats and future developments and update cybersecurity safeguards as needed.

For assistance with implementing cybersecurity safeguards, responding to cyber incidents and data breaches, drafting privacy, security and breach notification policies and procedures, or performing cybersecurity compliance training, please contact one of the attorneys listed below.

RICK HINDMAND

Read More

EMILY JOHNSON

Read More