HHS Issues Cybersecurity Guidance for Healthcare Organizations

Prepared by:
Kathryn Carey and Aleksandra Vold
BakerHostetler

LORMAN®
Published on www.lorman.com - May 2019

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

HHS Issues Cybersecurity Guidance for Healthcare Organizations

*Written by **Kathryn Carey** and **Aleksandra Vold** – 1/7/19*

BakerHostetler will post a series of blogs to fully explore the recommendations and guidance Health and Human Services provides healthcare organizations in its report.

Cyberattacks continue to rise across industries, and healthcare is no different. Eighty percent of U.S. physicians reported having experienced some form of cyberattack. In 2017, cyberattacks cost small and midsize businesses an average of $2.2 million, with 60 percent of small businesses going out of business within six months of the attack. According to a study from IBM Security and the Ponemon Institute, the cost of a data breach for healthcare organizations rose from $380 per record in 2017 to $408 per record in 2018, the highest cost for data breaches across all industries. In 2016, U.S. healthcare systems lost $6.2 billion due to data breaches. No doubt this amount continued to rise in 2017 and 2018, with the growing number of cyberattacks.

Against this backdrop, on Dec. 30, 2018, the Department of Health & Human Services (HHS) issued guidance on cybersecurity for healthcare organizations. The report — the work product of a task force created by the Cybersecurity Act of 2015 and composed of healthcare and

cybersecurity experts — evaluates current threats against healthcare and public health organizations, identifies common weaknesses within healthcare organizations, and suggests mitigation efforts.

HHS specifically states that the report is not "a de facto set of requirements that all organizations must implement." Rather, the report serves as guidance for organizations to customize cybersecurity practices based on the organization's size. This approach recognizes that an organization's size impacts many aspects of its operations, including its IT security capabilities, staffing, investment in IT security, number of affiliate entities and exchanges with other healthcare systems. The report cautions that identifying the size of an organization is not as simple as it may seem, and it provides a table to guide organizations in their evaluation.

The report is broken down into four sections:

1. The Main Report, which addresses current cybersecurity threats facing healthcare organizations, with the goal of raising general awareness of the issue.
2. Technical Volume 1, which guides small healthcare organizations on what to ask their IT security teams or vendors.
3. Technical Volume 2, which is intended for IT security professionals within midsize and large healthcare organizations.
4. Resources and Templates, which provides additional resources and references for healthcare organizations.

The report analogizes good cybersecurity practices with hand hygiene; just as healthcare professionals know the importance of handwashing

to stop the spread of germs, healthcare organizations need to practice good "cyber hygiene" to stop the spread of cyberattacks. Hospitals need to make good cyber hygiene a culture within their organizations, just as they have done with good hand hygiene.

To begin the process, organizations must understand the differences between a "threat" and a "vulnerability." A threat is something that has the potential to cause harm. A vulnerability is a weakness that may be exploited by a threat, resulting in harm or loss.

BakerHostetler's blog series will address each of the five threats explored in the Main Report:

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

By identifying your organization's vulnerabilities, and the threats that may exploit them, you can take appropriate precautions to lessen the chances of exploitation and, ultimately, harm or loss to your patients and organization alike. The Technical Volumes detail 10 practices to mitigate these threats, which the blog series will also discuss.