JANUARY 24, 2019

HHS RELEASES UPDATED GUIDANCE ON HEALTH INDUSTRY CYBERSECURITY PRACTICES

Cybersecurity continues to rank amongst the major concerns for health care providers. Long-term care facilities in particular are increasingly attractive "low-hanging fruit" for digital bad actors because of the misperception that smaller entities are not big enough to warrant the resources and risk associated with a cyberattack. With a new year, the Department of Health & Human Services Cybersecurity Act of 2015 Health Care Task Group published updated cybersecurity guidance to assist with cybersecurity preparations. The guidance, which is available here for review, includes:

1. **The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients**. This publication examines five current security threats, presents steps to mitigate those threats and provides an overview of the status of cybersecurity threats to health care providers.
2. **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations**. This publication emphasizes practices for smaller health care organizations with limited resources and access to a dedicated IT staff.
3. **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations**.This publication focuses on recommendations for medium and large health care organizations with multiple sites, dedicated IT staff and funding.
4. **Resources and Templates**.This publication contains resources such as the Practices and the NIST Cybsecurity Framework, Practices Assessment, Roadmaps and Toolkit to help implement recommended practices.

Health care providers need to be especially vigilant because their data is highly valued and their systems are critical to patient safety and care. Guidance such as this can be one tool in a provider's toolbox to address cybersecurity risk. These resources are written in "user-friendly" language and offer a starting point for long term care facilities to build internal discussions and practices around protecting sensitive information. These resources may be especially helpful for long-term care providers with limited resources to address cyber threats.

PRACTICAL TAKEAWAYS

- Leadership teams should review current policies and procedures and assess the recommended practices to ensure adequate plans are in place in the event of a cyberattack.
- Providers should consider cybersecurity as an element in the development of their emergency plans, risk assessments and annual training exercises. This may include consider adding cybersecurity protocols to their policies and procedures.

If you have questions about your cybersecurity processes, please contact:

- Ammon Fillmore at (317) 977-1492 or afillmore@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com;
- Sean Fahey at (317) 977-1472 or sfahey@hallrender.com;
- Your regular Hall Render attorney.