Preventing High-Tech Health Care Hacks: Federal Agencies Issue Ransomware Guidance for Health Care Providers

07.13.2016

One of the fastest-rising cyber threats to businesses of all kinds, “ransomware” has already affected several hospitals and health systems. For example, in March, we published an **Alert** on the attack on Hollywood Presbyterian Medical Center, which kept the hospital offline for 10 days. Ransomware is a type of cyberattack where a hacker enters into a network, encrypts the company’s data, and holds the data for “ransom.” The hackers make a monetary demand, and, if the victim pays, the hackers provide a decryption key for the victim to get back its data. In recognition of this serious threat to both patient data and patient welfare, Secretary Burwell of the Department of Health and Human Services (“HHS”) issued a letter on June 29, 2016, with accompanying interagency guidance on the threat and prevention of ransomware attacks.

The guidance provides an overview of what a health care entity can do with respect to prevention and response. It recommends several measures which should be “no brainers” for most health care providers, as many of the measures have been required, directly or indirectly, under the HIPAA Security Rule since its inception, including data backup, risk analysis, staff training, and incident response planning. The guidance also emphasizes training employees to be wary of suspicious links and emails, as typically the criminals initiate the attack through “spearfishing” emails designed to look legitimate. An entity should also restrict access based on user responsibilities and maintain and update effective spam filters, firewalls, and anti-virus and anti-malware programs.

If health care entities find themselves in the unfortunate position of being the subject of an attack, the agencies urge the entities to implement their incident response and business continuity plans, including immediate isolation of the affected machine or device. Entities are also instructed to contact the Federal Bureau of Investigation (“FBI”) or U.S. Secret Service. These agencies advise against paying the ransom, stating that it only encourages the criminals to attack others. Further, there is no guarantee that the affected entity will get the decryption key, and it may even be asked to pay more than the original ransom demand.

Ransomware and other cyberattacks are a more prevalent part of reality as health care goes high-tech. All health care providers and entities should seek to adopt appropriate prevention measures and have all necessary plans in place to respond efficiently in the event of an attack.

To read all of the details in the ransomware guidance, click **here**.

EVENT ANNOUNCEMENT:
"HIPAA Compliance: The Current Audit and Enforcement Environment"

Join us on Thursday, Aug. 4 for a seminar/webinar on "HIPAA Compliance: The Current Audit and Enforcement Environment."

This free program will feature Iliana L. Peters, J.D., LL.M., Senior Advisor for HIPAA Compliance and Enforcement at the HHS Office for Civil Rights, and members of Williams Mullen's Health Care Practice.

Topics:

- What do health care providers and their business associates need to know about HIPAA compliance?
- What are OCR HIPAA audits, and what should you do to prepare?
- What makes up OCR's enforcement muscle, and how have they been flexing it?

Attendees can participate in two ways:

1. **Williams Mullen's Richmond Office**
   Williams Mullen Center
   200 South 10th Street, 16th Floor
   Richmond, VA 23219
   (Williams Mullen attorneys will be presenting at this location. Iliana L. Peters will be participating via webinar.)
2. **Webinar**

For more information and to register, please click here.

Related People