HHS Releases Guidance for Health Industry on Voluntary Cybersecurity Practices

February 21, 2019

By John B. Waters, Counsel

The Department of Health and Human Services (HHS) has released a publication entitled the "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients." The HICP was prepared in response to the mandate set forth in the Cybersecurity Act of 2015 Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry. It provides voluntary cybersecurity practices for healthcare entities of all sizes.

The HICP describes five current major threats to the healthcare industry and recommends 10 cybersecurity practices to help mitigate these threats. The five major threats identified in the HICP and a description of each are as follows:

1. E-mail Phishing Attack - an attempt to trick someone in a healthcare workplace into giving out password or other sensitive information to a hacker using e-mail.

2. Ransomware Attack - installation of malicious software that denies access to data through encryption until the data's owner pays a ransom to the hacker to unlock the data.

3. Loss or Theft of Equipment or Data - such as the theft of a laptop containing medical records.

4. Insider, Accidental or Intentional Data Loss - such as someone impersonating a medical professional by telephone to gain access to a patient's medical records.

5. Attacks Against Connected Medical Devices That May Affect Patient Safety - such as a hacker taking control of medical devices such as heart monitors and causing them to power off or continuously reboot.

The HICP is comprised of four volumes. The main volume of the HICP gives many helpful tips to minimize the cybersecurity risks described above. Two technical volumes are included in the HICP that are written for IT professionals. Technical Volume 1 focuses on cybersecurity practices for small healthcare organizations, and Technical Volume 2 focuses on practices for medium and large healthcare organizations. Each Technical Volume sets forth the following ten practices with implementation recommendations to mitigate such threats:

1. E-mail protection systems;

2. Endpoint protection systems;

3. Access management;

4. Data protection and loss prevention;

5. Asset management;
6. Network management;
7. Vulnerability management;
8. Incident response;
9. Medical device security; and
10. Cybersecurity policies.

The final volume provides guidance and templates that healthcare organizations can use to assess their existing cybersecurity policies and procedures and to develop or enhance those policies and procedures.

According to the HICP, the average cost of a data breach for a health care organization was $2.2 million and the per health care record cost of a data breach was $408. Because of the potential for physical and financial harm to patients and financial harm, loss of reputation and legal exposure to healthcare providers resulting from a data breach, the HICP should be thoroughly reviewed by healthcare providers and their IT support personnel to assess and update their existing cybersecurity policies and procedures.

For more information on the legal requirements relating to healthcare data privacy, the penalties and other legal consequences that are applicable to unauthorized disclosures of protected health information and methods for mitigating such adverse consequences, please consult the following individuals at Roetzel:

Ericka Adler
Manager
312.582.1602 | eadler@ralaw.com

Avery Delott
312.582.1636 | adelott@ralaw.com

David Hochman
312.582.1686 | dhochman@ralaw.com

Christina Kuta
312.582.1680 | ckuta@ralaw.com

Lee Levin
312.580.1248 | llevin@ralaw.com

John Waters
312.582.1685 | jwaters@ralaw.com