March 30, 2016

OCR Cyber-Awareness Monthly Update

March 2016 Topic: New Cyber Threats and Attacks on the Healthcare Sector

Recent cyberattacks on major health care entities have been eye-opening for some healthcare professionals and have changed many views on security for the healthcare sector. In the past, security compliance personnel and their leadership at health care entities may have been more focused on issues like security breaches that involve workforce members losing unencrypted laptops or other mobile devices containing patient's protected health information. While lost or stolen devices still represent a large portion of health-industry breaches, healthcare sector organizations must consider new cyber threats, as well.

Cyber threats and attacks can disrupt healthcare entities information systems and cause delays in patient care. For example, certain attacks can slow down the process of: providing patients their daily medication or meals; printing patients' labels, ID badges, discharge papers; and accessing patient medical records. Some attacks can affect life-saving medical devices. Attacks can also cost healthcare entities an enormous amount of money if they feel pressured to pay a ransom demand to a group of hackers, to restore their information systems that contain patient health information and are needed to provide proper patient care, and to pay costs associated with a breach.

Cyberattacks involving hackers attacking the databases and network systems of healthcare sector organizations are becoming more common and sophisticated, and may be different from the privacy breaches many entities have seen previously.

Covered entities and business associates should be aware of these new types of cyberattacks:

- **Nation-State Attacks** – Healthcare entities may be the target of hackers in China, Russia, and several countries in Eastern Europe. The motivation for this type of attack varies from collecting protected health information for sale and collecting data for intelligence-building and potential espionage, to stealing intellectual property from medical technology companies.

  The FBI website provides a few precautions covered entities and business associates can take to protect sensitive data:
  - Recognize internal and external security threats to your entity's sensitive data.
  - Identify your entity's sensitive data and implement a plan for safeguarding it.
  - Secure physical and electronic versions of your entity's sensitive data.
  - Confine your entity's sensitive data to a need-to-know basis.
  - Provide training to employees about your entity sensitive data security plan.

- Do not store private information vital to your entity (e.g., trade secrets, business plans, etc.) on any device that connects to the Internet.
- Use up-to-date software security tools.
- Educate employees on e-mail tactics such as spear phishing. Establish protocols for quarantining suspicious e-mail.
- Remind employees of security policies on a regular basis through active training and seminars. Use signs and computer banners to reinforce security policies.
- Ask the FBI or other security professionals to provide additional awareness training.

Resources:
Federal Bureau of Investigation (FBI):
https://www.fbi.gov/news/stories/2012/november/teaching-industry-how-to-protect-trade-secrets-and-national-security/teaching-industry-how-to-protect-trade-secrets-and-national-security - *(Steps to guard against nation-state attacks)*

- **Ransomware Attacks** – Hackers and ransomware tools are becoming more sophisticated. The main objective in using ransomware is to destroy backups of files and databases that contain electronic patient health information and to encrypt and lock up files and databases that contain ePHI in order to charge covered entities and business associates hundreds to thousands of dollars to unlock the data.

US-CERT and CCIRC recommend healthcare entities and business associates to take the following preventive measures to protect their computer networks from ransomware infections:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Data should be kept on a separate device, and backups should be stored offline.
- Maintain up-to-date anti-virus software.
- Keep operating system and software up-to-date with the latest patches.
- Do not follow unsolicited web links in emails.
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

The Federal Bureau of Investigation encourages healthcare entities and business associates not to pay the ransom, as this does not guarantee files will be released. Any instances of cyber fraud should be reported to the FBI.

Resources:
United States Computer Emergency Readiness Team (US-CERT):
https://www.us-cert.gov/ - *(Ransomware remediation)*

Federal Bureau of Investigation (FBI): https://www.fbi.gov/scams-safety/fraud/internet_fraud - *(Report internet fraud)*

- **Smartphone Attacks** – Attacks on smartphones may be involved in more covered entity security breaches in the near future. Patients, staff, and third-parties of covered entities are using smartphones to interact with new healthcare applications and medical devices.

Although smartphones have beneficial features, entities must ensure these devices have appropriate safeguards against cyberattacks.

According to US-CERT, in order to reduce the consequences of a cyberattack on smartphones the following security practices should be taken into consideration by healthcare entities and business associates:

- When choosing a mobile phone, consider its security features. Ask the service provider if the device offers file encryption, the ability for the provider to find and wipe the device remotely, the ability to delete known malicious applications remotely, and authentication features such as device access passwords.
- Configure the device to be more secure. Enable the password feature on mobile phone and choose a reasonably complex password. Enable encryption, remote wipe capabilities, and antivirus software if available.
- Do not follow links sent in suspicious email or text messages.
- Limit exposure of your mobile phone number, by carefully choosing which public websites on which to post mobile phone numbers.
- Carefully consider what information you want store on the device.
- Be choosy and do a little research on mobile applications before installing them. Check what permissions the applications require. If the permission seems beyond what the application should require, do not install the application.
- Maintain physical control of the devices in public or semi-public places.
- Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi-Fi.
- Set Bluetooth-enabled devices to non-discoverable.
- Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots.
- Delete all information stored in a device prior to discarding it.

Resources:
United States Computer Emergency Readiness Team (US-CERT):
https://www.us-cert.gov/ - *(Smartphone security practices)*