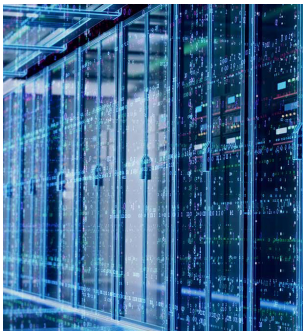
5 CYBERSECURITY THREATS TO FOCUS ON



HHS publication provides an easy-to-understand approach designed for health care entities

While the issue of cyber liability is something medical providers have been warned about for years, the question of "where to start" to protect yourself can be complicated. Earlier this year, the Department of Health and Human Services released a publication titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" to help medical practices and facilities prioritize what issues to tackle first.

Based on recommendations that focus on the most impactful threats, the publication notes that "Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry must make cybersecurity a priority and make the investments needed to protect its patients…Hackers look for targets that require the least time, effort, and money to exploit. Do not make the mistake of thinking that your practice, no matter how small, is not a target for indiscriminate cyber-attacks."

The most impactful threats the publication identified are:

1. Email phishing attack
2. Ransomware attack
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

The HHS publication includes a two-page summary regarding each threat with real-world scenarios, quick tips, and a table that outlines vulnerabilities, impact, and practices to consider. We have selected two of the five threats to highlight in this newsletter as an example of the useful information available in the HHS publication.

THREAT: Email Phishing Attack

REAL-WORLD SCENARIO: Your employees receive a fraudulent email from a cyber-attacker disguised as an IT support person from your patient billing company. The email instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.

Vulnerabilities

- Lack of awareness training
- Lack of IT resource for managing suspicious emails
- Lack of software scanning emails for malicious content or bad links
- Lack of email detection software testing for malicious content
- Lack of email sender and domain validation tools

Impact

- Loss of reputation in the community (referrals dry up, patients leave)
- Stolen access credentials used for access to sensitive data
- Erosion of trust or brand reputation
- Potential negative impact to the ability to provide timely and quality patient care
- Patient safety concerns

Practices to Consider

- Be suspicious of emails from unknown senders, emails that request sensitive information such as PHI or personal information, or emails that include a call to action that stresses urgency or importance
- Train staff to recognize suspicious emails and to know where to forward them
- Never open email attachments from unknown senders
- Tag external emails to make them recognizable to staff
- Implement incident response plays to manage successful phishing attacks
- Implement advanced technologies for detecting and testing email for malicious content or links
- Implement multifactor authentication (MFA)
- Implement proven and tested response procedures when employees click on phishing emails
- Establish cyber threat information sharing with other health care organizations

COPIC TIP: 5 CYBERSECURITY THREATS TO FOCUS ON

THREAT: **Insider, Accidental, or Intentional Data Loss**

REAL-WORLD SCENARIO: An attacker impersonating a member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the patient's health record.

Vulnerabilities

- Files containing sensitive data accidentally e-mailed to incorrect or unauthorized addressees
- Lack of adequate monitoring, tracking, and auditing of access to patient information on EHR systems
- Lack of adequate logging and auditing of access to critical technology assets, such as e-mail and file storage
- Lack of technical controls to monitor the e-mailing and uploading of sensitive data outside the organization's network
- Lack of physical access controls
- Lack of training about social engineering and phishing attacks

Impact

- Accidental loss of PHI or PII through e-mail and unencrypted mobile storage, resulting in reportable data breaches
- Reportable incidents involving patients who are victims of employees who inappropriately view patient information
- Financial loss from insiders being socially engineered into not following proper procedures
- Financial loss due to an employee inadvertently giving an attacker access to banking and routing numbers because the attacker used a phishing e-mail disguised as originating from the bank
- Patients given the wrong medicines or treatment because of incorrect data in the EHR

Practices to Consider

- Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors
- Implement and use workforce access auditing of health record systems and sensitive data
- Implement and use privileged access management tools to report access to critical technology infrastructure and systems
- Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads

In addition to the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" publication, there are two supporting technical volumes that outline ten cybersecurity practices for managing the key threats (one volume is designed for small health care organizations, the other is for medium to large organizations). There is also a "Resources and Templates" document that includes a variety of cybersecurity resources and templates for end users to reference.

All of these materials are available for download at:
www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx