Cybersecurity issues: threats, risks, resources

Q Where can my OMS practice learn more about cybersecurity risks, and what resources are available?

A The HHS Office of Information and Security established the 405(d) program and task group, a collaborative effort to align healthcare industry security approaches. The program and task group work to develop best practices and resources to help those in the healthcare industry face current cybersecurity risks. Available resources include templates, tool kits, fliers, posters, newsletters and webinars.

View and download these resources at 405d.hhs.gov.

Q What are the top cybersecurity threats facing the healthcare industry and OMS practices?

A "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients" – available at 405d.hhs.gov/Documents/HICP-Main-508.pdf – outlines the top five threats that might impact a practice and provides real-world scenarios showing how each threat could occur within a practice.

- Email phishing: An email used to trick the recipient into sharing personal information.
- Ransomware: Occurs when hackers gain control of data or a computer and hold the information for ransom.
- Loss or theft of equipment: Laptops, smartphones and thumb drives can be lost or stolen and could end up with hackers.
- Insider, accidental or intentional data loss: An attacker with internal access to technology infrastructure, network or databases collects patient data either accidentally or intentionally.
- Connected medical devices: A phishing attack that affects a server connected to medical devices, such as a heart monitor, can give a hacker complete control of the medical device and risk patient safety.

For additional resources on how to reduce cybersecurity threats, visit 405d.hhs.gov.

Q Are there certain best practices that should be followed to protect OMS practices from cybersecurity threats?

A Technical Volumes 1 and 2 of the HICP publication provide 10 best practices for small and large healthcare organizations:

- Email protection systems – Instill basic email protection controls such as antispam and antivirus and implement education and awareness activities for employees.
- Endpoint protection systems – Endpoints include connected hardware devices – desktops, laptops, mobile devices. Remove excess administrative accounts and conduct regular patching.
- Access management – Establish unique accounts for all users, limit the use of shared accounts and implement a multi-factor authentication.
- Data protection and loss prevention – Implement proper data protection and loss prevention education within the practice and prohibit the use of unencrypted storage devices.
- Asset management – Keep an accurate inventory and establish policies for properly disposing of retired assets.
- Network management – Secure the network with network segmentation, intrusion prevention, physical security and guest access.
- Vulnerability management – Detect potential technical flaws with routine vulnerability scans and patching.
- Incident response – Before a cybersecurity incident occurs, establish an incident response plan to know who will lead the investigation and what steps will be taken.
- Medical device security – In addition to following HICP's best practices, consider adding security terms to medical device contracts.
- Cybersecurity policies – Establish and implement cybersecurity policies, procedures and processes for the practice. Be sure to include the roles and responsibilities and ongoing education and awareness for staff.

To download the complete HICP technical volume, visit 405d.hhs.gov. ■