How to Implement Patching

Patching for Medium-sized Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is patching?
Patching is regularly updating your systems by applying security updates provided by the software or device manufacturer.

Why is it important?
Patching your systems is important because it removes vulnerabilities that can be exploited by attackers.

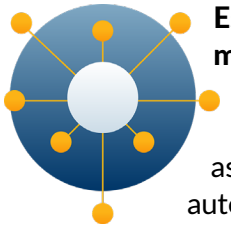
How will this keep my organization safe?
Each patch modifies a software application, rendering it more difficult for hackers to maintain programs that are aligned with the most current version of that software application.

Patching Mitigates:

- Ransomware
- Insider, Accidental, or Intentional Data Loss
- Attacks against connected medical devices that may affect patient safety

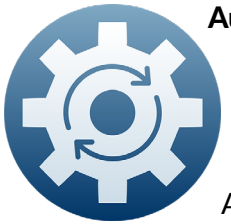
Implementation Tips:

Maintain a current inventory of all software on endpoints. This will facilitate complete and consistent maintenance and patching to protect against client-side attacks. Ensure that you train your workforce on the need to report any lost or stolen endpoints to your cybersecurity department. Reporting should occur promptly so cybersecurity departments can execute the proper incident response procedures.



Establish an endpoint management system. Device management systems, which connect to IT devices such as endpoints and servers, can automate the management and maintenance of these assets. They are highly effective at executing tasks such as software discovery, patch management, and performance monitoring.

Distribute Operating Systems patches during regular maintenance times. Apply security patches at designated system down times. This will ensure the flexibility to remove a patch that is not compatible with your network. This ensures your resources are continually available and prevents service interruptions in your day-to-day operations.



Automatically update and distribute patches to third-party applications. Include those known to be vulnerable, such as Internet browsers Adobe Flash, Acrobat Reader, and Java. Applications or information systems that support business processes, such as third-party applications, should be prioritized when automating a patch schedule to prevent externally facing software from causing additional vulnerabilities in your network.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*