



# PRESCRIPTION:

## Vulnerability Management

Vulnerability management is the process used by organizations to detect technology flaws that hackers could exploit. This process uses a scanning capability, often provided by an EHR or IT support vendor, to proactively scan devices and systems in your organization.

***Protect yourself and your patients by following the course of treatment below:***

### For Small Organizations:

- Schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws.
- Conduct web application scanning of internet-facing web servers, such as web-based patient portals. Specialized vulnerability scanners can interrogate running web applications to identify vulnerabilities in the application design.
- Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, and always patch critical vulnerabilities within 14 days.

### For Medium/Large Organizations:

*In addition to instituting the tips for Small Organizations be sure to incorporate the following:*

- Implement Host/Vulnerability Endpoints Scanning. In this model, vulnerability scanners are leveraged to identify weaknesses in OS or third-party applications that reside on endpoints and servers.
- Utilize strict configuration management and change management procedures. Also, a testing plan should be part of the change management process. It should include a vulnerability scan of new network connectivity (such as a firewall change) or a new system function or service.
- Establish a routine of penetration testing. These types of tests are sometimes called red teaming; the goal is to actively exploit your own environment before malicious actors do.

*For more Vulnerability Management practices, please visit [405d.hhs.gov](http://405d.hhs.gov) to download a copy of the HICP technical volume for your organization. Check out the available resources 405(d) has to offer by visiting our social media pages @ask405d on Facebook, Twitter, and Instagram!*