WINDOWS 7 SUPPORT IS ENDING SOON: UPGRADE NOW TO PROTECT YOUR PRACTICE

OVERVIEW

Keeping computer software updated with the newest security updates is critical to system security. Microsoft recently reminded users that Windows 7, one of its most-used operating systems, will no longer be supported as of January 14, 2020. This means that security updates for Windows 7 will no longer be issued. Many clinicians use Windows 7 in their practices, underscoring the critical importance of this announcement to the health care industry.

If your practice is running Windows 7, your practice and patient information may be at risk. It's important that you take action by upgrading to a supported operating system before January 2020. If your practice currently uses Windows 7, you might consider an upgrade to Windows 10. Read this for information on how to check if your current technology is Windows 10-compatible.

Under Ontario's *Personal Health Information Protection Act*, all health information custodians (HICs) have a legal obligation to safeguard against unauthorized, collection, use and disclosure of patient personal health information. Ensuring practice technology and software is current and up to date is one important step in meeting this obligation.

The Ontario Medical Association is working to find practical solutions that further support physicians and their practices from cyber threats. One such pilot project is currently underway involving Cylance anti-virus detection software. The pilot involves 100 general practitioners, specialists and residents. An update on the outcome will be provided in the fall.

UNDERSTANDING PRACTICE TECHNOLOGY

The technology used in medical practices is vital to the administration of patient care. As clinicians continue to onboard and acquire new digital health tools, it's imperative that they understand the technology they own and how to best maintain it. Over the last decade, the adoption of medical technologies has skyrocketed, including the use of an Electronic Medical Record (EMR). To ensure that there are no disruptions in the use of these technologies, both hardware and software need to be maintained and updated on an ongoing basis. When these technologies have not been maintained, the risk in becoming vulnerable to being exploited increases and may put patient care at risk as well.

Using an operating system that is no longer vendor-supported can increase the risk of cyberattack. The 2017 WannaCry ransomware attack compromised more than 300,000 machines in approximately 150 countries. Most affected computers were running Windows 7, which malicious actors were able to exploit in this quick-spreading attack.

The first step to protecting one's practice is understanding what technology is used.

HARDWARE

All technology begins with hardware. In a clinical practice, hardware typically includes computers (laptops, servers, etc.), and the network infrastructure (internet router, network switches, Wi-Fi, etc.) needed to communicate between computers and externally to the internet. Hardware can be complex to set up and maintain, so it is helpful to consult with a professional IT organization to manage, audit and monitor a practice's technology. Practices should also consider other hardware devices such as smart phones and other portable devices that may not be included in a professional IT organization's service agreement. These devices must also be updated and protected if they are used to provide patient care.

SOFTWARE

Software includes applications, scripts, and programs that run on hardware. Software frequently used by clinicians and their staff include operating systems (Microsoft Windows, MacOS, etc.), internet browsers (Firefox, Chrome, Internet Explorer, etc.), and their EMR. Operating systems support a computer's basic functions. It is important to ensure that the operating system version being used includes the latest updates provided by the supporting software company/vendor. These updates typically provide performance improvements, bug fixes and security patches, and help prevent hackers from gaining backdoor access to computers and other devices. However, as new versions of operating systems are released, technology companies eventually stop supporting older versions – as Microsoft is doing with Windows 7.

Other installed software programs, including virus detection software and firewalls, also require attention and upgrades. Often, this is accomplished simply by downloading an update; in other cases, the software may require an upgrade to the latest version.

Cloud-hosted software solutions must also be properly maintained and supported. For example, EMR vendors with OntarioMD-certified EMR Offerings are expected to maintain and upgrade their Offerings based on requirements published in the EMR Hosting Specification. This specification defines the set of vendor expectations for software, hardware, and processes.

IS YOUR SYSTEM UP TO DATE?

To reduce the risk of unwanted IT events, your practice management policies must include a plan for regular updates to the hardware and software used by your practice, to ensure all applicable vendor-issued system and security patches are integrated.

IT and EMR maintenance needs can be overwhelming for a busy practice. Hiring an IT professional will help ensure your practice technology stays up to date. OntarioMD is also here to support you, whether you have just started using an EMR or have used one for many years. You can connect with an OntarioMD Practice Advisor for advice any time at support@ontariomd.com.

For feedback or inquiries regarding this bulletin please contact us at support@ontariomd.com.

The views expressed in this publication are the views of OntarioMD and do not necessarily reflect those of the Province. Nothing in this bulletin should be construed as legal advice or a substitute for consultation with your legal representatives.
Copyright © 2019 OntarioMD. All Rights Reserved