Growing HIPAA Threat – Ignore Windows XP at Your Own Peril

Blog  |  May 21, 2013  |  EHR, HIPAA, Health IT, Law & Malpractice
By Marion K. Jenkins, PhD, FHIMSS

"Advance Directive:" If HIPAA Security, ICD-10, EHR updates, and the explosion of mobile applications were not enough for you to worry about from a health IT standpoint, you need to be very concerned about a real danger that is likely lurking throughout your facility — computers and servers running old versions of Microsoft operating systems. In most cases these are definitely DNR (Do Not Resuscitate) issues.

"How long do I have, doctor?" Starting in less than a year, April 8, 2014 to be exact, Microsoft will no longer provide any support whatsoever for Windows XP, which was the most ubiquitous desktop and laptop operating system in Microsoft's history, with hundreds of millions of copies sold since 2001. That means that in less than a year from now, security updates and virus patches will cease. That means that practices will be in a real threat to viruses, Trojans, and other security vulnerabilities, because all the bad guys in cyberspace know that millions of computers will be unpatched. Those practices that do not take action will become an easy target for back-doors and other entry points on millions of networks around the world.

And in early 2015, Microsoft Server 2003, which also currently runs on millions of servers, will also stop getting any patches or updates.

"How widespread is the disease?" Even though Microsoft stopped selling Windows XP nearly 5 years ago, recent studies have shown that the percentage of active devices running Windows XP is still nearly 40 percent, just slightly behind the numbers for Windows 7, and those numbers have remained nearly constant for the last several months. Exact figures are not readily available on how many actual devices are represented, but we have observed that nearly every medical facility has multiple instances of Windows XP and/or Server 2003 running within their environments. Some of these devices are still running simply because no one has gotten around to finding and upgrading them, but many are running critical applications that cannot be upgraded for one reason or another.

Server 2003 was replaced about 5 years ago by Server 2008, but here again there has been a very slow migration away from Server 2003, and it is believed that there are millions of servers still running Server 2003.

"What's the prognosis?" The obvious implication is that all workstations and laptops running Windows XP will become non-compliant with HIPAA no later than April of next year. HIPAA Security Rule section 164.308(a)(5)(ii)(B) states that you must implement "procedures for guarding against, detecting, and reporting malicious software." Obviously if you cannot update your software to protect your systems against malicious software, it is impossible for you to comply with this HIPAA Security Rule specification.

"Is there a cure?" Yes, but like most life-threatening conditions, early detection and prompt action is critical. This sounds like these deadlines are a long way off, but they are right around the corner from an IT perspective. First, if you have systems running Windows XP and/or Server 2003, you probably have other operational and HIPAA Security issues as well. You need to have a thorough review and inventory of all your IT systems, listing risks and vulnerabilities. This is actually required action anyway for ARRA/HITECH/meaningful

http://www.physicianspractice.com/blog/growing-hipaa-threat-ignore-windows-xp-your-o...
use, as well as HIPAA Security Rule compliance. Even if you have done it for Stage 1 of the meaningful use requirements, you are required to do it again for Stage 2. And HIPAA Security requires "periodic updates," which most experts agree should be at least annually. Second, you need to upgrade your systems to not only satisfy HIPAA but to take advantage of much more scalable and secure IT infrastructure, such as virtualization and medical-grade cloud hosting. These more advanced solutions cost far less than before, and provide much greater capabilities and improved performance.

Addressing Windows XP and Server 2003 issues will not only make your practice more functional and secure, but it will satisfy HIPAA and meaningful use requirements. And it won't make you the giant target for hackers, because they will find those systems still running Windows XP and Server 2003 much easier prey.