SEMEL CONSULTING HIPAA Brief

Why you should Replace Windows XP & Office 2003 by April 8, 2014

No HIPAA or Meaningful Use Compliance with XP

UPDATE: A $ 1.7 million breach penalty issued by the Office for Civil Rights on April 22, 2014, substantiates our opinion that (a) just listing something in a risk analysis is not sufficient and (b) having most systems safe with others recognized as risks is not acceptable.

In an interview with Healthcare Info Security, IT security expert Kevin Fu, University of Michigan professor and member of the NIST Information Security and Privacy Advisory Board, warns that "threats change very quickly in the internet. New malware is being born all the time, but now there is not going to be any kind of Microsoft update available when the problems arise…When malware gets into a Windows XP machine, which can be a medical device, it's often a silent infection. You don't notice; there's no blinking light on the medical device saying [it's] infected. Instead what might happen, and what has happened, is the device slows down. It may begin to give false readings. So if it is a sensor device, it may start to give erroneous information to the healthcare professional. I'm aware of some products where health records from two different patients are getting accidentally merged by some corrupted pieces of software, and if you add malware into the mix, it doesn't exactly bring much confidence."

On April 8, 2014, Microsoft is ending security updates and patches for Windows XP and Office 2003. Because it will be defenseless, just having a Windows XP computer on your network will be a HIPAA violation— which also makes you non-compliant with Meaningful Use. Windows XP will be a time bomb that could easily cause a reportable and expensive breach of electronic Protected Health Information (ePHI.) HIPAA fines and loss of Meaningful Use money can far outweigh the expense of replacing your old computers. Even newer machines will be at risk if you use Microsoft Office 2003.

The HIPAA Security Rule requires that you protect patient information. Without system patches and updates, which will not exist for Windows XP after April 8, this will be impossible with Windows XP. .NIST guidance goes into more detail.

Some XP defenders have used this FAQ answer from the Office for Civil Rights that the HIPAA Security Rule does not mandate specific operating systems to claim that continued use of Windows XP is allowable.

> *The Security Rule does not specify minimum requirements for personal computer operating systems, but it does mandate requirements for information systems that contain electronic protected health information (e-PHI).. the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications …Additionally, any known security vulnerabilities of an operating system should be considered in the covered entity's risk analysis (e.g., does an operating system include known vulnerabilities for which a security patch is unavailable, e.g., because the operating system is no longer supported by its manufacturer).*

This is not the sole guidance on protecting health information, and should not be taken alone because HIPAA also requires Risk Management of vulnerabilities identified in the Risk Analysis. What often are ignored by those wanting to keep Windows XP are the rest of the HIPAA Security Rule, the HIPAA Omnibus Final Rule, Meaningful Use requirements, and HIPAA enforcement penalties. These must all must be considered *together* when protecting health information. For example, if you list an unsupported operating system as a vulnerability then you must define how you will implement effective risk management to protect patient data. This will be impossible for organizations that want to keep Windows XP and also must comply with HIPAA.

The HIPAA Security Rule is all about implementing effective risk management to adequately and effectively protect EPHI.

National Institute of Standards and Technology (NIST)

To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

Meaningful Use Office of the National Coordinator for Health Information Technology

What Experts Say

Continuing to use Windows XP after (April 8, 2014) will magnify security risks and associated mitigation costs, considerably… Because of ever-advancing threats, the risks of continuing to use obsolete (and soon unsupported) software are unacceptable.

US Information Security and Privacy Advisory Board

Without critical Windows XP security updates, your PC may become vulnerable to harmful viruses, spyware, and other malicious software which can steal or damage your business data and information. Anti-virus software will also not be able to fully protect you once Windows XP itself is unsupported. Microsoft

Running XP SP3 (or lower) and Office 2003 after the end of support date may expose the company to potential security and compliance risks. Worth consideration is also fact that aside of vulnerable systems it is expected for several third party software vendors to stop support of their applications on XP Platform after April 2014 as well – this adds additional danger of vulnerable applications and multiplies the possible infection vectors. Symantec Corporation

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes… after April 8, 2014, any machine—physical or virtual—running the Windows XP operating system with access to FBI CJIS data will result in a noncompliance finding during an audit.

FBI, Criminal Justice Information Services (CJIS) Security Policy

The Electronic Health Records Incentive Program **'Meaningful Use' guidance requires that you:**

- *review all electronic devices that store, capture, or modify electronic protected health information*
- *comply with HIPAA*
- *continue to review, correct or modify, and update security protections*
- *correct any deficiencies (identified during the risk analysis) during the reporting period*
- *review and update the prior analysis for changes in risks*

HIPAA enforcement activities also stress the requirements to identify threats and implement security measures.

(Hospital) did not fully evaluate the likelihood and impact of potential risks to the confidentiality of ePHI … implement appropriate security measures to address such potential risks, document the chosen security measures and the rationale for adopting those measures, and maintain on an on-going basis reasonable and appropriate security measures.

OCR $ 1.5 million HIPAA penalty Case Resolution

Security patches and updates are a critical security measure to protecting patient data.

The Massachusetts Institute of Technology (MIT) IT department made patching Number One in its Top Ten Safe Computing Tips:

Patch, Patch, PATCH!

Set up your computer for automatic software and operating system updates. An unpatched machine is more likely to have software vulnerabilities that can be exploited

Because patches and updates will no longer be available, Texas A&M University has banned Windows XP computers from campus after April 8.

> ***Microsoft is discontinuing support of Windows XP on April 8, 2014. After this time, Windows XP systems will no longer be allowed on campus. All exceptions must be approved. If you need to request an exception, send email to (Chief Information Security Officer) describing the justification for the exception and compensating controls. No systems running XP will be approved for firewall port openings.***

You need to take replacing Windows XP and Office 2003 seriously.

Act quickly. On April 8 both will become defenseless and subject to the will of hackers. The deadline not only affects health care, but every business and government agency, which is likely to result in a shortage of equipment and delays getting replacement systems installed. It may take weeks or months to order equipment and get it installed, after you have gone through your purchasing process.

Getting rid of Windows XP means replacing both hardware and software. Consider replacing desktops with laptops, micro PC's that mount to the backs of monitors, all-in-one computers, thin clients without hard drives, or tablets.

Look at the new ways to purchase or 'rent' a replacement for Office 2003. Rather than installing and supporting software on every device, you can pay low monthly fees for the latest software through the Cloud, where everything is accessed through the Internet. Talk to an IT professional to determine what will work best for you. Be sure you only consider vendors that will sign HIPAA Business Associate Agreements and validate to you that they comply with HIPAA. (Any breach they cause may be your responsibility.)

Replacing Windows XP lets you comply with both the HIPAA and Meaningful Use requirements that you secure patient data. Whatever computers you decide to buy must include business-class operating systems that include features to secure access and protect data. 'Home' operating systems do not have security features that can protect patient data. You must have a professional version of Windows that includes security features and can join a domain.

Don't think that all your protected patient data is in your EHR system. It may be all over your office on individual PCs. Data should not be stored on PC's because it makes it harder to comply with HIPAA and to secure and back up everything. Have a professional IT specialist set up your network so data is always stored on a secure server that is backed up offsite. A network with a server as a domain controller will also enable you to comply with HIPAA's requirements for secure access and retaining access logs for six years.

Some of your Windows XP computers may be managing diagnostic or special purpose devices, and are not managed as part of your office network. Don't let these hide from you as you replace your office systems. They all need to go. Many diagnostics tools from imaging to dental to ophthalmologic devices have dedicated Windows XP computers that came with the device and are supported by that vendor. Talk to the vendor now. Hospitals may have Windows XP computers connected to point-of-sale systems in Admissions, the billing office, cafeterias, and gift shops.

Encryption is now included in some business-class versions of Windows. It can also be purchased separately from vendors like WinMagic, Symantec, and McAfee/Intel Security. Encryption should be installed on every computer that stores any patient data, including servers, desktops, laptops, and portable devices. Encryption not only protects data at a high level than passwords, it exempts you from reporting a lost or stolen device. Considering the recent $ 1.5 million fine for a lost laptop, $ 1.7 million fine for a lost hard drive, and $ 150,000 fine for a lost thumb drive, encryption is your cheapest insurance against a reportable data breach.

Doctors aren't IT professionals any more than IT professionals are doctors. Refer yourself to a specialist. Your office is not your home. Just because they may function does not mean you can use the same consumer grade computers, software, and networking devices that would work in your home.

The HIPAA and Meaningful Use requirements that you protect patient data require business-class solutions installed by qualified IT professionals. Protecting patient data requires a professional knowledge of IT security. Devices that include security features must be properly installed, configured, and actively maintained.

The IT industry term for Wellness is Managed Services. IT companies use sophisticated automated tools for remotely monitoring the performance and security of your network. This can help you comply with HIPAA's requirements for monitoring access to data and ensuring your security stays in place. Find an IT professional that can provide Managed Services and is certified in HIPAA.

SEMEL CONSULTING

www.semelconsulting.com

About the Author (Author Profile)

Mike Semel is certified in HIPAA and has been the CIO for a hospital (Covered Entity) and has provided IT support for healthcare providers (as a Business Associate.) Mike is certified in Business Continuity planning and helped develop the CompTIA Security Trustmark. Semel Consulting offers a managed compliance service called HIPAA SOS, compliance audits, Meaningful Use Security Risk Analysis, and business continuity planning. Visit www.semelconsulting.com or more information.

This article was originally published at www.4medapproved.com/hitsecurity

Semel Consulting works with IT resellers and their vendors to develop HIPAA compliance programs