Will Windows XP violate HIPAA as of 4/8/14??

Many small providers and practices are worried about pricey computer & software upgrades and data migration costs if using XP becomes a HIPAA violation on 4/8/14.

Here’s the deal

Windows announced that it will stop supporting the operating system Windows XP after 4/8/14 (including security patches). While the HIPAA Security Rule does not specifically require particular supported operating systems, “Unsupported and unpatched environments are vulnerable to security risks. This may result in an officially recognized control failure by an internal or external audit body, leading to suspension of certifications, and/or public notification of the organization’s inability to maintain its systems and customer information.” (Microsoft)

Does the government address this issue?

The US Department of Health & Human Services (HHS) addresses the issue directly on their website (click here) and says: “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).

Therefore, as part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.

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).”

How do you avoid a HIPAA violation?

This means that, while it’s not a HIPAA violation to use Windows XP after 4/8/14, you must address the threats in your risk analysis. This means that you know what can happen and have a plan to minimize the risk (described in the risk analysis). This plan should include a timeline to
move away from Windows XP in the future, because it’s not sustainable to continue using that operating system indefinitely. However, this does give you a little time to slowly changeover, minimizing the potential financial impact.

**When does using XP become a HIPAA violation?**

Continuing to use Windows XP after 4/8/14 (or other unsupported operating systems) becomes a HIPAA violation if it’s not addressed in your security risk analysis. As the risks increase over time, you are obligated to keep the risk analysis updated. Eventually, you do need to switch to supported operating systems, and it removes the burden of worrying if you’re in violation of HIPAA!

For more information, see [HHS Security Rule Guidance](http://www.hhs.gov). (Source: CDA)

**Interested in moving your business away from XP?**

Windows XP is two, soon-to-be three, generations behind current modern operating systems. In non-IT terms, that’s like trying to maintain an antique automobile in the age of electric cars. Sure it’ll get you around, but the cost to keep it operating will overtake the cost of simply upgrading.

Unquestionably, you should replace your XP computers one-for-one with new PCs with a current generation operating system. The most recent release of Microsoft Windows is 8.1, but Windows 7 is still the preferred platform in a business environment. Most resellers will offer Windows 8 or 8.1 with a new PC, but include a license to downgrade to Windows 7 for free.

But if the timing isn’t right for your company to make that kind of investment, you may want to consider virtual desktop infrastructure or VDI. For most clients, this doesn’t require any new hardware: you simply repurpose your existing PCs with an up-to-date operating system that utilizes shared server resources. In the event that you want or need to buy new hardware, for as low as $350 you can get a thin client that will give you access to your desktop in the cloud. And, it’s all powered by the latest Microsoft Server 2012 technology, which means your XP End of Life worries are a thing of the past.

If you are interested in exploring virtual desktop options, we invite you to contact our partner MTG.