Published on *The National Law Review* https://natlawreview.com

Is Your Health Insurance Portability and Accountability Act (HIPAA) Compliance Program Going Out the Window with XP?

Article By:

Dianne J. Bourque

Cynthia J. Larose

April 8, 2014 marks the end of Microsoft's support for the Windows XP operating system, which means the end of security updates from Microsoft and the beginning of new vulnerability to hackers and other intruders into systems still utilizing the operating system. But does the end of Windows XP support mean that HIPAA covered entities and their business associates using Windows XP are automatically out of compliance with HIPAA as of April 8th? Not necessarily.

It is impossible to say with certainty that April 8th equals HIPAA non-compliance for XP users. There is no one-size-fits-all answer as to whether or not continued use of XP will result in a HIPAA violation, because there is no one-size-fits-all approach to compliance with the HIPAA Security standards. HIPAA Security standards are "flexible and scalable" to ensure that each regulated entity may implement security measures that are reasonable in light of the size and complexity of the organization. As a threshold matter, users of Windows XP must determine whether or not **electronic protected health information or ("ePHI")** even passes through an affected system. XP users should also evaluate whether or not there are compensating security measures to protect ePHI or whether additional security measures could be implemented to temporarily protect ePHI, such as disconnecting affected computers from the internet.

However, Microsoft has been sounding the warning bells about the end of support for Windows XP for quite some time now: "We just did not know" likely casts doubt on whether your organization has been sufficiently diligent. The official End of Life Information Center has some good baseline information. The issue becomes that there will be no patches or updates provided by Microsoft – including security patches – from today forward. Section 164.308(a)(5)(ii)(B) of the Security Rule requires "procedures for guarding against, detecting and reporting malicious software." If you are not receiving security patch updates, you will be exposed to "zero-day" threats.

- Figure out the scope of the problem, and look carefully at your IT infrastructure and architecture.
- Identify dependencies: what runs on Windows XP and why

- Upgrade each machine and make sure that any software and/or lab equipment is likewise updated.

- At least install the final Windows XP update NOW so that your machines start their unsupported lives protected from the most recent known vulnerabilities.

In short, Windows XP users should do what all HIPAA covered entities and business associates should do when there is a significant change in operations or the environment presenting new threats or vulnerabilities to ePHI: they should update their HIPAA risk assessments and remediate identified gaps in security*. Note: regulated entities in need of risk assessment assistance should refer to our recent post on the Office for Civil Rights new automated risk assessment tool.* Windows XP users should also begin planning migration to a new operating system, if the process has not already begun.

National Law Review, Volume IV, Number 98