Report on Patient Privacy Volume 20, Number 2. February 06, 2020 With Support Gone for Windows 7, Patches, Other Steps Now Required

By Jane Anderson

Microsoft Corp.'s decision to end support for its popular but aging Windows 7 operating system (OS) opens up additional privacy, security and patient safety vulnerabilities in the health care sector, which already is notoriously slow to update operating systems on computers and devices, security experts say.

Support and security patches for Windows 7 ended on Jan. 14, meaning Microsoft won't fix security flaws that are identified. This is significant, since Windows 7 is widely used in health care, including within medical devices that may be implanted in patients, says Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor.

"With an OS as popular as Windows 7, this creates a huge population of cybervictims [hackers] can target," Herold tells *RPP*.

Dealing with this problem is not as simple as updating the operating systems, since many of the medical devices in question can't even run newer operating systems. Roger Shindell, president and CEO of Carosh Compliance Solutions, notes that many devices were developed on older operating systems and some are not supported any longer, so it's not possible to patch known vulnerabilities.

"Health care tends to have the highest rate of the legacy Windows 7 machines and other legacy operating systems, including those on [Internet of Things] medical devices," adds Michelle O'Neill, director of corporate compliance at Summit Health Management in New Jersey. "These are often connected to a network and give the health care sector great exposure. The reality is that health care entities need to update and phase out many of the devices, but the challenge is that it's not always practical from a financial perspective."