

## Outpatient Facility Coding Alert

### Technology: Plan Ahead to Ensure Your Facility Stays Compliant After Computer Security Changes

#### Windows XP shift could jeopardize your HIPAA compliance.

When someone mentions HIPAA security, you probably think about whether your paper files are under lock and key, whether your record destruction practices measure up, or whether your passwords are strong enough to keep others out of patient information. But you may be overlooking a small, yet troublesome, security measure that could cost your facility in a big way.

Find out why keeping up with computer software security patches is critical for, not only your practice's efficiency, but also to avoid violating HIPAA security protocols.

#### Focus On the Requirements

Although the HIPAA Security Rule doesn't mandate the type or version of operating system your practice must install on its computers, you do need to be sure that if the system contains or has access to electronic protected health information (e-PHI) there are some things you need to do.

According to the Department of Health & Human Services (HHS) HIPAA frequently asked questions (FAQ) website, "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)."

**What it means to you:** "As a healthcare organization, HIPAA compliance involves protecting patient records," explains **Candice Ruffing, CPC, CENTC, CPB**, coding supervisor, IT coordinator, and compliance officer at South Coast Ear, Nose & Throat in Port St. Lucie, Fla. "According to the HIPAA Security Rule section 164.308 (a)(5)(ii)(B), organizations must implement procedures for detecting, guarding against, and reporting malicious software."

#### Keep Systems Compliant With Patches

One easy way to ensure your system stays secure and HIPAA compliant is to install security patches and updates from the software manufacturer.

"Software updates, also known as 'patches' or 'service packs' are computing data that improve usability, performance, and security vulnerabilities within a piece of pre-existing software," Ruffing explains. "It is important to keep the patches and updates current to ensure a safe environment for medical records. By not paying attention to these critical updates, they can create a HIPAA violation if your PCs or servers are targeted by a virus or malware."

#### Beware of Future Windows XP Issues

Right now, many consultants and practices are buzzing about the fact that Microsoft is going to stop supporting Windows XP in April of this year. That means practices running Windows XP will no longer have security patches to install to keep their systems secure.

**Official word:** According to the Microsoft website, "After April 8, 2014, Microsoft will no longer provide security updates

or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. PCs running Windows XP after April 8, 2014, should not be considered to be protected, and it is important that you migrate to a current supported operating system — such as Windows 8.1 — so you can receive regular security updates to protect their computer from malicious attacks."

"If a healthcare organization chooses to use Windows XP, attackers can easily find, exploit, and access patient records ... if healthcare providers fail to migrate away from Windows XP they won't be able to protect their systems against malicious activity," Ruffing warns.

**The problem:** For a facility that is running Windows XP on multiple systems, upgrading the software on every computer may be too costly. The process may also take an extensive period of time as a practice cannot easily transition all computers at one time.

Ruffing started inventorying her practice's systems and software as soon as she read about the upcoming security support elimination in August 2013. Based on her experience, Ruffing suggests starting as soon as possible if your practice needs to make upgrades. "Our upgrade to HIPAA compliance for a four physician, two nurse practitioner (NP), four audiologist (AuD) practice cost \$38,000.00+ for the upgrade of our equipment," she adds.

**Best bet:** Check your systems and see if the lack of Windows XP updates — or any other security issues — will soon set your facility up for HIPAA problems. If the answer is yes, be proactive and develop a plan for correcting the problems as soon as possible.

Performing a risk assessment for any security issues is an important practice for any healthcare entity. Checking your computer systems for vulnerabilities — present or future — should be part of that process.

**Read more:** You can visit [www.microsoft.com](http://www.microsoft.com) for further details about the Windows XP transition.