HARRISBIOMEDICAL™
COMPLIANCE SERVICES
1035 ANDOVER PARK WEST, SUITE 120, TUKWILA, WA 98188

Windows XP Support has Ended!

***"As of April 8, 2014, support and updates for Windows XP
are no longer available. Don't let your PC go unprotected.***

On April 8th Microsoft pulled the plug on the support system for XP. The XP operating system is almost 14 years old and, according to MS and the computing world, it hasn't aged well. It's been rife with problems from the get-go and Microsoft has issued over 1000 patches since its debut, along with "years of on-going support and constant updates" to plug the holes in the security system.

According to the techno experts, even with more than a decade of security fixes, XP remained fundamentally flawed and insecure.

The issue - at its root and as it relates to protecting patient information - is that if the security system is flawed, a practice can't protect patient information as required under HIPAA. And, if it's not protected (secured), it must be considered vulnerable to attack and access by persons not authorized for that access (hackers, etc.).

If and when unauthorized access to ePHI occurs, it is considered a breach of confidentiality and the practice could be in serious trouble (Skagit County (Washington) Health Department just wrote a $215,000 check for - among other things - failing to secure patient information). The XP system simply can't stand up to modern day security threats. The Microsoft message is, *"Unless you want your data stolen, your network hacked, or your computer taken over to be used as a slave to send spam, you need to get off this creaky platform."*

This is why the IT experts are telling their clients they ultimately could be in trouble. Without the constant fixes, patches and support from Microsoft (which as of April 8th ceased), it could be just a matter of time before something bad (PHI breach) happens. Some clients were concerned that their IT guys were just trying to sell them a new system. According to everything that's out there, that's probably pretty good advice if they are banking on the XP security system.

The fact is that "*every standard desktop-security risk that a computer faces will be amplified, because there are no fixes being written by Microsoft."* Understanding that "given", there are a few things published that might help folks decrease their exposure if they have to keep using an old XP machine.

1. Talk to and listen to your IT expert. She/he is there to help you until you can make the transition to a safer operating system,
2. Update your software. It's important that antivirus, firewalls, and browsers are up to date, along with Java, Adobe, Office and other common infrastructure apps,
3. Bar browsing and emails on company computers. Since most attacks come via email and the web it makes sense to eliminate these vectors on XP devices,
4. Restrict connectivity. The network is a prime route for attacks on vulnerable systems; disconnecting XP devices entirely from the network is the best option,

5. Encrypt your patient connected emails. If you emails are encrypted they are secured and protected to the degree established by HIPAA, (If it's encrypted, it's secure),

6. Encrypt all devices, including desk top computers and all mobile devices such as laptops, I-pads, I-phones, discs, tapes, USB/flash drives on which patient protected information (PHI) is used or stored. Devices get stolen and password protection is never enough. (If it's encrypted, it's HIPAA compliant),

7. Monitor your system on a very regular, scheduled basis to identify and track any unauthorized access and/or activity (HIPAA requirement),

8. Back up your dental/patient software (required by HIPAA) daily and store off site. Encrypted cloud services are available and very affordable).