Introduction

As widely publicized, Microsoft has ended support for Windows XP as of April 8, 2014. This document describes the impact of that decision, if any, on your Elekta products that may use Windows XP inside, and what Elekta has done and will do to ensure the same secure and reliable user experience that we always aim to provide. The document is formatted as 'Frequently Asked Questions', to which we provide answers. These answers are not for a specific product, but describe the overall Elekta policy around Windows XP.

What does the end of support for Windows XP mean? Will I be able to use my system?

Microsoft has provided support for Windows XP for the past 13 years, but as of April 8, 2014 technical support, which includes *automatic security patches*, ended. The licenses will be kept live and functional until December 2016 though, so you can use your equipment until then.

So I will be able to use my license but will not be getting security patches for Windows XP; that still sounds worrying. Does it mean that my Elekta equipment is unsafe now?

No. Installation of Microsoft patches is normally regarded as good practice for your personal computers, to protect against threats such as viruses that a user could come across in email or when surfing the web on their personal computer. However, for *medical systems* this approach is not the first line of defense. Medical systems are required to undergo extensive testing in a known configuration before they can be released for clinical use. It is for this reason that Elekta has never recommended applying newly released patches until they have been fully tested for use in a clinical environment in combination with our equipment. (In fact, for many of our products we explicitly say one must not install patches).

OK, that makes sense but is there a possibility of getting malware (virus) on my system now? What are the risks?

First of all, malware is very unlikely to result in a *safety* issue (trigger radiation for example). The main concern of the presence of malware would be a loss of *reliability* or loss of patient data.

Also, it is important to understand that the way malicious code can be spread is by opening specially crafted attachments in an email, a malicious website or by executing code from other distribution media such as CD/DVD or USB devices. Elekta products themselves have an architecture that makes malicious access to patient information very unlikely. The Elekta medical applications are all unique and have different functionality, but when at all possible the systems are designed with an extensive list of built-in safeguards.

For further information, see Elekta Software Security Statements:
http://www.elekta.com/healthcare-professionals/products/elekta-software/product-security-statements.html

So what do you recommend I do?

Generally, we recommend that you start transitioning your Elekta Software product to a more updated version supporting an operating system such as Windows 7.

In the case where transitioning is not yet possible, you can keep using Elekta products safely and effectively with the following recommendations. Many of these recommendations are good security best practices and have nothing to do with Windows XP. It is beneficial to overall system and data security to implement them and keep them in place even after systems have been migrated to a supported operating system.

Elekta recommends that you use a secured VLAN, with only the Treatment Delivery Suite computers connected such as Integrity, XVI, iViewGT or the Treatment Control station of our afterloaders. Only the applicable ports required for operation such as the DICOM interface should be allowed to be configured. The Network Security Solution (NSS) provides this capability.

- Only software provided by Elekta should be installed on the computers provided as part of the Treatment delivery suite.
- These treatment delivery systems should not be used to access email, nor untrusted websites.
- Except for Neuroscience solutions anti-malware scans are permitted (out of clinical hours) from a computer on the same network. This can be achieved using the NSS for some products (no anti-malware software is installed on the control system). For Neuroscience, anti-malware scans are not done. Instead these systems contain white list based anti-malware solutions that prevents all non certified programs from executing.
- Make sure that regular backups of the systems are taken.
- All computers are at risk of malware contamination from external storage devices and media, for example CD-ROM, DVD-ROM, USB hard disks, and USB flash memory drives. Elekta recommends that you examine storage devices and media for malware and remove the malware before you use the device or media on a computer.
- Continually perform a risk analysis of your HIPAA security rules as part of your security management processes and implement addtionnal safeguards if required. A U.S. government guideline on HIPAA in relationship to computer operating systems is provided below.

Does the end of support for Windows XP pose a risk to HIPAA compliance?

It is Elekta's analysis that the end of support for XP does not impact HIPAA compliance. This is backed up by the following statement from HHS and the fact that no known vulnerabilities exist that, as stated before, could pose a safety threat or compromise patient data. The highlighting in the passage was done by Elekta for your convenience.

"HHS HIPAA FAQ - Security Rule

Does the Security Rule mandate minimum operating system requirements for the personal computer systems used by a covered entity?

Answer:

No. The Security Rule was written to allow flexibility for covered entities to implement security measures that best fit their organizational needs. 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)."

Where can I get more information regarding which products (and their versions) need upgrading?

Please, contact your respective sales representative. They will be able to provide this information.