Microsoft End of Support for most Windows 7 and Windows Server 2008 R2 Products

Introduction

As widely publicized, Microsoft will end support for most Windows 7 versions as of January 14th 2020. In addition, Microsoft will also end support for Windows Server 2008 R2, which is used to host some versions of Monaco, ABAS, and Direct Access. For some specific versions of Windows, e.g. Windows Embedded Standard 7 (WES 7), that are also used in Elekta Products, this date is different and we refer to another letter (Windows WES 7 End of Support statement, Document #45133711281) for more information. This document describes the impact of that decision, if any, on your affected Elekta products 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 7 and Windows Server 2008 R2 products.

What does the end of support for Windows 7 and Windows Server 2008 R2 mean? Will I be able to use my system?

Microsoft has provided support for these product versions for many years, but as of January 14th 2020 technical support, which includes *automatic security patches*, will end.

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

No, your Elekta equipment is safe. 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 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 product to a version that supports an operating system such as Windows 10. In case this is not yet possible, you can keep using Elekta products safely and effectively with the following recommendations. Many of these recommendations are best practices and are not related to Windows 7 or Windows Server 2008 R2 products. It is beneficial to overall system and data security to implement them and keep them in place after systems have been migrated to a supported operating system.

Elekta recommends that you use a secured VLAN, with only the 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 configured. The Elekta Network Security Solution (NSS) provides this capability or it can be configured in the local firewall software.

- Only software provided by Elekta should be installed on the computers provided as part of the Linac Delivery Suite
- These treatment delivery computers should not be used to access email or the internet.
- Except for Neuroscience solutions anti-malware scans are permitted (outside 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 Brachytherapy it is allowed to run anti-malware software on the Treatment Control stations and Treatment Planning systems. See the product manuals for the specific configurations. For Neuroscience, anti-malware scans are not done. Instead these systems contain white list based anti-malware solutions that prevent all non-certified programs from executing.
- Make sure that regular backups of the databases and systems are taken and that these are stored in a secure location. Check the product manuals for specific recommendations.
- 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.
- For Brachytherapy a USB drive can be used to export a plan from the Treatment Planning System to the Treatment Control system in case of network problems. We strongly recommend to use a dedicated USB drive for this and examine the USB drive for malware contamination on regular basis.
- Continually perform a risk analysis of your HIPAA security rules as part of your security management processes and implement additional 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 7 and Windows 2008 Server R2 pose a risk to HIPAA compliance?
It is Elekta’s analysis that the end of support does not impact HIPAA compliance. This is backed up by the following statement from the U.S. Department of Health and Human Services (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 Health Insurance Portability and Accountability Act (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 service representative. They will be able to provide this information.