The GxP Implications of Windows 10 End-of-Life for Pharma Labs

Windows 10, the commonly used operating system in pharmaceutical laboratories, is reaching its end-of-life (EOL). The EOL deadline, imposed by Microsoft, has significant operational implications for companies in all sectors and industries. In the pharmaceutical industry, there are additional GxP (Good Practice) implications that must be addressed.

And there is no time to delay, as the first major Windows 10 EOL deadline is rapidly approaching. There are immediate things you can do to buy some additional time, but these solutions are temporary. Therefore, it's essential to develop and implement a plan to migrate the Windows 10 devices in your pharma lab to Windows 11.

Contents: A GxP Guide to Windows 10 EOL for Pharma Labs

Windows 10 EOL Explained

Why is Windows 10 EOL?

The simple answer to why Windows 10 is EOL is that Microsoft has developed and launched an upgraded version of its flagship operating system. Windows 11 comes with new features, including AI-focused functionality. Microsoft has switched its attention completely to Windows 11, and it wants users to make the switch too.

When Is the Windows 10 EOL Date?

The Windows 10 EOL date is October 14, 2025.

What Does Windows 10 EOL Mean for Pharmaceutical Companies?

Windows 10 EOL means that, after October 14, 2025, Microsoft will stop providing support as standard for Windows 10. This means no functionality updates, feature improvements, or, crucially, security updates. As well as performance and security implications, **Windows 10 EOL also has significant compliance implications for pharmaceutical companies**.

Sample Risk Assessment Template: Windows 10 EOL

Risk Area	Description	Impact	Likelihood	Risk Level	Mitigation
Security vulnerabilities	Loss of vendor support may expose systems to unpatched vulnerabilities	High	High	High	Migrate to Windows 11 utilizing ESUs if this can't be done before the deadline
Data integrity	Corrupted or lost data due to the unsupported operating system	High	Medium	High	Validate all critical data migration steps; ensure backups
Software compatibility	Existing GxP apps may not function on the new operating system	Medium	Medium	Medium	Verify compatibility; update software versions where needed
Business continuity	Unexpected downtime or operational delays during migration	High	Low	Medium	Create a rollback plan; conduct testing in a sandbox environment
Regulatory non-compliance	Audit finding for use of unsupported operating system in validated systems	High	High	High	Include an operating system migration plan; document decision-making and approvals

WESTBOURNE
Global IT Solutions

Why is this EOL Deadline Different from Other Microsoft EOL Deadlines?

It is common for Microsoft to have a defined support cycle for its products, with EOL dates published regularly. The fact that Windows 10 will soon be EOL is not, in itself, unusual.

The main reason why Windows 10 EOL is different from other EOL deadlines is because of the hardware requirements of Windows 11.

Windows 11 has very specific hardware requirements that even relatively modern PCs don't live up to. This means you can have newish PCs in your pharmaceutical laboratory that still work well but are not compatible with Windows 11.

One of the main sticking points is a piece of hardware called a TPM 2.0 chip.

What is a TPM 2.0 Chip – A Techie and Non-Techie Explanation

Let's start with the non-techie explanation. TPM stands for Trusted Platform Module. It is a security chip in modern PCs, but they come in different versions. TPM 2.0 is the minimum requirement for Windows 11. **If your PC has an older TPM chip or no TPM chip at all, you can't upgrade it to Windows 11**.

If that's all the info you need, you can skip to the next section on the GxP implications of Windows 10 EOL.

For the technically minded, here is a more detailed, albeit brief, explanation. TPM 2.0 security chips are integrated into a computer's motherboard or processor. They serve as a secure storage for cryptographic keys, passwords, and other sensitive data. This means they ensure the integrity of the system's boot process, and they authenticate users. TPM 2.0 chips also protect data by creating a secure environment that's resistant to tampering.

TPM 2.0 offers enhanced security and cryptographic flexibility compared to TPM 1.2, the previous version. TPM 2.0 supports newer algorithms like SHA-256 and RSA-2048. It also offers more flexibility with key management and algorithm choice, making it more robust for modern security standards. TPM 1.2, while functional, is more limited in terms of supported algorithms and security features.

Most importantly, TPM 1.2 is not compatible with Windows 11.

What are the GxP implications of Windows 10 EOL?

Overview of the GxP Implications of Windows 10 EOL

GxP regulations, such as those under FDA 21 CFR Part 11 and EU Annex 11, require pharmaceutical companies to ensure the computer systems used in regulated

environments remain secure, reliable, and compliant. Windows 10 EOL has significant GxP implications:

GxP Requirement	Windows 10 EOL Impact	Remediation
Security & data integrity	No security updates, increased risk	Migrate to a supported operating system (OS); use ESUs temporarily
Regulatory compliance	Potential audit failures, non-compliance	Document risk, plan OS migration, validate changes
System reliability	Higher risk of failures, no support	Upgrade hardware/software, validate the environment

Security Risks

After the EOL date, Windows 10 will no longer receive security patches or bug fixes from Microsoft. This leaves systems vulnerable to new threats, making it impossible to guarantee data integrity, confidentiality, and availability. All three are key GxP requirements.

Compliance Risks

Operating unsupported systems can result in failed audits as regulators expect up-to-date, supported, and secure platforms. Continued use of Windows 10 after the EOL date could lead to findings of non-compliance during inspections.

Data Integrity and Availability

Data integrity and availability are essential in GxP, with GxP guidelines emphasizing the need for a reliable and secure IT infrastructure. Unsupported systems increase the risk of data breaches or loss, directly impacting data integrity and system reliability.

What Are Extended Security Updates?

Overview of Extended Security Updates

Extended Security Updates (known as ESUs) are a temporary and limited Windows 10 EOL lifeline. Microsoft launched ESUs at least partially in response to the slower-than-expected uptake of Windows 11.

In other words, ESUs are a halfway house, letting Microsoft stick with its originally published EOL deadline while also giving customers, especially enterprise customers, a bit more time to plan and implement the migration.

What Do You Get with an ESU License?

With ESU licenses in place, the Windows 10 devices in your pharmaceutical laboratory will receive security updates from Microsoft.

It's important to emphasize that ESUs only provide you with security updates. There will be no new features for Windows 10.

What Do ESUs Cost?

According to Microsoft, **the cost for ESU licenses is USD $61 per device**. This is only the year one cost, though. Microsoft says the price will double in year two and double again in year three.

How Long Can I Use an ESU License?

Providing you pay for annual licenses, you can use ESUs for three years. After three years, Windows 10 will be well and truly dead and buried, with no further security updates provided by Microsoft.

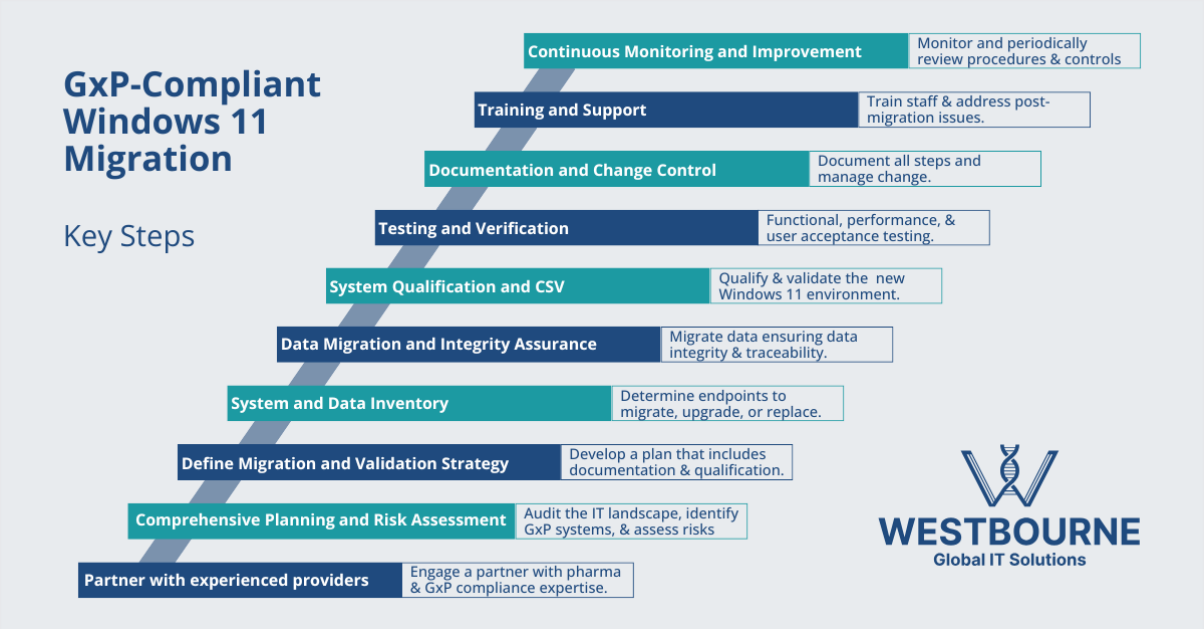
What Does Windows 10 EOL Really Mean for Pharmaceutical Companies?

The bottom line with Windows 10 EOL is that you will have to migrate endpoints in your pharmaceutical laboratory to Windows 11. While there are alternatives to buying new equipment (such as VDI solutions), it is likely that new PCs will be needed that meet the system requirements of Windows 11.

The arguably more important part of the process than purchasing new PCs is planning and implementing the migration. Migration strategies and processes are important in all industries and types of businesses, but in the regulated sector, they are even more critical because of the validation and regulatory considerations that are involved. For pharma labs that are part of high-speed, high-volume manufacturing facilities, minimizing downtime is also crucially important to ensure production targets are maintained.

Windows 11 Migration Strategy: An Overview for Pharmaceutical Companies

Key Steps in a GxP-Compliant Windows 11 Migration



Migration Planning

Regulators expect pharmaceutical companies to proactively plan for technology lifecycle changes. Transitioning to a supported OS (such as Windows 11) is the most effective way to maintain GxP compliance.

Before initiating the migration, it is essential to conduct a system inventory and compatibility assessment across all IT assets, particularly those used in GxP-regulated environments. This includes identifying legacy PCs, systems integrated with lab instruments, and any endpoints that may not meet Windows 11 hardware requirements.

As per FDA and EU GMP expectations for system lifecycle management and change control, this assessment is a foundational step to ensure that all impacted systems are identified, prioritized based on risk, and appropriately managed within the migration and validation plan.

ESUs

For systems in your pharmaceutical facility that cannot be migrated by the deadline, especially validated systems, Microsoft's ESU program offers temporary security updates. As mentioned above, each endpoint will need a separate ESU license.

It’s important to emphasize that this is a short-term, risk-managed solution and not a substitute for a full migration. Full migration will still be needed.

To ensure compliance, the use of ESUs should be justified with documented risk assessments and mitigation plans.

Validation and Change Control

Migrating to Windows 11 constitutes a significant change in most pharmaceutical IT environments, particularly where validated systems are involved.

Under GxP guidelines, this typically requires initiating a formal change control process, including documented impact assessments, updated validation plans, and execution of IQ/OQ/PQ protocols where necessary. In some cases, full revalidation may be triggered, especially if the operating system change affects application performance, data integrity, or integration with laboratory instruments.

This is important because regulators expect documented evidence that any changes to validated environments are assessed, controlled, and tested to ensure continued compliance with 21 CFR Part 11 and EU Annex 11. Skipping this step or applying a one-size-fits-all approach can result in data integrity risks, audit issues, or non-compliance during inspections.

Windows 11 Migration Compliance Responsibilities

Microsoft provides the technical controls and documentation for compliance, but ultimate responsibility for GxP compliance, including validation, governance, and ongoing risk management, remains with you as the regulated company.

GxP Compliant Windows 11 Migration Checklist

GxP-Compliant Windows 11 Migration Checklist for Pharmaceutical Companies

1. Planning & Governance

- [ ] Form a cross-functional migration team (IT, QA, CSV, business)
- [ ] Identify all GxP-relevant systems running Windows 10
- [ ] Define the scope and objectives of the migration project
- [ ] Establish a timeline considering the October 14, 2025 EOL deadline
- [ ] Inform regulatory stakeholders, if needed

2. System Inventory & Classification

- [ ] Document all systems (hardware and software) using Windows 10
- [ ] Classify systems by GxP impact: High / Medium / Low
- [ ] Identify third-party applications that may require revalidation

3. Risk Assessment

- [ ] Perform a risk assessment for continued use and migration
- [ ] Include security, data integrity, business continuity, and compliance risks
- [ ] Document risk mitigation strategies

4. Validation Strategy

- [ ] Determine if revalidation is required (full or partial)
- [ ] Create/update validation documentation including:
  - [ ] Validation Plan
  - [ ] Requirements Traceability Matrix (RTM)
  - [ ] IQ/OQ/PQ protocols
- [ ] Execute validation activities and obtain QA approval

5. Testing & Qualification

- [ ] Perform OS installation and configuration testing (IQ)
- [ ] Conduct operational testing (OQ) for system functionality
- [ ] Validate performance in a controlled environment (PQ)

6. Documentation Updates

- [ ] Update SOPs, user manuals, and training materials
- [ ] Revise system configuration and validation documentation
- [ ] Archive documentation per data retention policies

7. Training & Change Control

- [ ] Train users on the updated system or interface
- [ ] Initiate a change control record for traceability
- [ ] Review change control with QA and obtain approval

8. Post-Migration Review

- [ ] Conduct a post-migration review or audit
- [ ] Monitor system performance and GxP compliance
- [ ] Finalize and close change control

WESTBOURNE
Global IT Solutions

Download checklist PDF <note: this will link to a downloadable version of the checklist>

Conclusion: Start Planning Your Windows 11 Migration Now

Continuing to use Windows 10 after the EOL date creates significant compliance and security risks for companies in the pharmaceutical industry. **Migrating to Windows 11 with proper validation and change management is essential to maintain GxP compliance and ensure ongoing regulatory readiness**.

We can support your ongoing compliance and Windows 11 migration efforts. At Westbourne, we have technical, validation, and pharmaceutical industry expertise to help you put in place a temporary ESU-backed solution in addition to planning and implementing a full migration to Windows 11. Please get in touch with us today to speak to one of our migration experts.