Data Security Standard 8
Unsupported systems

The bigger picture and how the standard fits in

2018
## Contents

### Overview

- Software can live for forever, however…  

### Know your IT estate (all of IT)

- IT estates  
- Survey tool  
- Know your boundaries  
- Cooperation with other parties  
- Clinical applications and devices  
- Mobile devices  
- Remote locations

If your organisation has multiple locations which share a computer network see the General Guidance on data security standard 8.

- Managed estates  
- Make a list  
- Risk assessment  
- Un-upgradeable devices or software  
- The myth of a standalone PC or network  
- A moving target  
- Have a plan for updates

### Appendix 1 -

- Table of Data Security and Protection Toolkit Standard 8 Assertions

### Appendix 2 -

- Useful resources

### Appendix 3 –

- The National Data Guardian Reports
Overview

The NDG’s review data standard 8 states that:

“No unsupported operating systems, software or internet browsers are used within the IT estate.”

Systems, software or internet browsers which are no longer updated by their creators are called “unsupported”. There is a clear recognition that not all unsupported systems can be upgraded, and that financial and other constraints should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It’s about demonstrating that analysis has been done and informed decisions were made.

It is recognised that many social care organisations will not use IT extensively or that it might only be used in certain parts of the organisation and this guidance has been written with that in mind.

For organisations who use a large amount of IT – particularly groups – it may be useful to look at the general guidance for data security standard 8 as this has more information on dealing with an IT estate.
Software can live for forever, however….

Software, being digital, does not degrade over time, however it does become unsupported and therefore potentially vulnerable. Most of the widely available commercial software will have a support cut-off date. Once software is no longer supported, it is called “unsupported software”. Unsupported software is no longer “patched” by the software owner. This means that it will no longer have security updates and that any bugs will not be fixed.

The ramifications of using software beyond its support date will vary from recently retired popular operating systems with a significant risk, to a small bespoke package with a lower risk.

Generally, software will go through three phases:

- active: current product fully supported and patched e.g. Windows 10
- limited: still patched for security though maybe not functionality e.g. Windows 7 (extended support ends 14th January 2020)
- retired: system is unsupported and you should migrate. e.g. Windows XP and Vista
Know your IT estate (all of IT)

IT estates

An “IT estate” is the name for all of the digital systems within your organisation. IT estates come in all shapes and sizes and are as diverse as the many organisations in the health and care system. They range from large centrally supported single sites, to sites spread across a geographic area with local management, to a one building estate with a single PC in the back office.

Even in the smallest of estates, it can be a challenge to know all the applications installed on all the devices across that estate. A survey tool can help automate that task.

Think about the pieces of IT you have in your organisation and find out what operating system it is running and make a note. This can normally be found in your computer settings. For example, a desktop computer or laptop might have a Windows 7 or MacOS Sierra operating system.

Once you have done this consider what pieces of software you use on that machine. For most care providers this may include some or all of the following:

- payroll software
- rota software
- email software
- Microsoft Office / iWork
- care planning software
- training software
- HR software.

Survey tool

You should use a survey tool to take an inventory of your hardware assets and the software that resides upon them. You should then be able to reference the versions of software installed. For each piece of software, there will be a known supported version(s) and when which version(s) are end of life.

Generally, the survey tool will gather hardware and software assets to populate and update an asset database. The asset database can also have manually added / updated assets for those not detected.

Supported version of software are those that the manufacturer supports with patching and upgrades. It is not necessarily the latest version of the software.

End of life software is not updated or patched and therefore can be vulnerable to exploits with no cure.

Technology can be a key enabler when it proves to be effective in supporting staff to work simply and safely. The Review heard that in contrast, technology can become a source of risk when it is out of date and unsupported.

NDG Data Security Standards Report
Even with a small IT estate, it can be laborious to document software manually and keep track of it.

For the more common pieces of software, the software tool should report back whether it requires a patch or upgrade and it could be used to implement it.

Beware of the limitations of your chosen tool(s), for example, survey tools may not be able to track installed software.

These can be classified as IT assets management tools.
Know your boundaries

Understand the boundaries of your digital estate and do not over step them.

Ultimately you should know where your responsibilities end and another organisation’s begin. Consequently, you shouldn’t scan or try to update assets that are beyond your boundary.

If you use the Health and Social Care Network (HSCN), then you should not scan over it without consulting NHS Digital prior to doing so. Some vulnerability scanners (dependent on how aggressively or passively they are being used) can be indistinguishable from a cyber-attack.

Cooperation with other parties

You might not be able to upgrade some software yourself – for example, software bought from a third party.

It is possible that there is some software which you use which will only work on older operating systems and so you cannot update your operating system.

In either instance, you must talk to the supplier to try and find a solution.

Where there is no resolution with the supplier or a fix is unable to be applied (due to financial, license or technical reasons), the system should be risk assessed, reviewed and treated where possible.
Clinical applications and devices

You may have monitoring devices or other clinical devices around your organisation which also contain software which may be vulnerable.

A clinical device such as an ambulatory device or patient monitoring devices may look very different from computers or a phone, but at their core they can have pieces of software just as vulnerable as that on other devices.

Mobile devices

Understand and have a list of what mobile devices (smart phones, tablets or laptops) you have and how they are updated.

Remote locations

Some organisations operate over several locations (for example, care home chains, supported living locations). If your organisation has several locations, the ones which are not your head office are sometimes called “remote locations”.

If your organisation has multiple locations which share a computer network, see the General Guidance on data security standard 8.

Managed estates

You may decide that it is easier to employ external IT support in order to keep track of this for you. In this case, they might be able to assist with this part of the Toolkit.

Generally, it will be expected that your supplier runs the tool on your behalf (and undertakes any necessary remediation with your approval). They provide you with a copy of the results and come back with any issues for your determination.

Make a list

From these steps, you should be able to compile a list of all of the software that you use. A list from your survey tool should be compiled. It is very likely (unless you have a small IT estate with standard software only) that the survey tool will not capture every piece of software on every device.

In both cases, manual intervention may be required to add that software or devices
**Risk assessment**

If you discover that you have unsupported software but cannot update it, you should ensure that this is risk assessed.

Make a record of why you are not upgrading, i.e. too expensive, it will stop another piece of vital software from working etc. Ensure that you also record what mitigations you are putting in place to protect the data which is held on this system. This risk assessment should be signed off by the most appropriate person in your senior management team (this might be the SIRO) and a record should be kept.

**Un-upgradeable devices or software**

Dealing with software or devices that cannot be upgraded or patched will be difficult if it is still required and cannot be replaced. In these circumstances, it should be treated as an obsolete system that is unmanaged or untrusted (see Appendix A guides)

MANDATORY - What software do you use?

Data Security Standard 8.1.1
The myth of a standalone PC or network

One of the common myths in social care is that having one PC connected to the internet is a standalone PC as it is not on a network with other PCs.

The types of terms used are:

- “It is on a standalone network, it doesn’t need to communicate with anything else.”
- “It’s a standalone PC, it’s only connected to the internet, not any network.”
- “It’s that old a piece of software, nobody would ever hack it.”

It is just as vulnerable as any other PC on a big internal network.
A moving target

Much like any product with a defined life, if you are replacing products towards the end of their support window with the next newest product, this may be midlife itself and be approaching its own retirement. This scenario is true with products such as Windows, where there are currently three versions within their support lifecycle.

Consequently, it is important to treat discovery and treatment as a continuous cycle.

Have a plan for updates

“Patching” or “patches” is another word for “updating”. You should have an effective plan or strategy for implementing patches on a regular basis. For many organisations, this might just be a case of allowing automatic patching (where your computers automatically update themselves).
Sometimes staff can prevent automatic updates from happening because they are inconvenient. You should check to make sure that this isn’t happening and try to schedule when the updates will happen. You can schedule updates in your computer settings.

It is important with automated patching that you follow up on any issues (such as where a patch cannot be applied to a specific desktop). It is also good practice to verify your results, you can do this with a product such as vulnerability scanner. There are vulnerability scanners freely available online.

If you have an external IT support company, they should be able to do this for you.

Make sure you record what your policy is and keep it with your other policies and procedures.

An example patching policy is in Appendix 2: Patching guidance for health and care organisations: NHS Digital good practice guide. Note that this guidance is aimed at larger organisations with a significant IT estate.
## Appendix 1 - Table of Data Security and Protection Toolkit Standard 8 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Mandatory</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 All software has been surveyed to understand if it is supported and up to date.</td>
<td>Yes</td>
<td>8.1.1</td>
<td>What software do you use?</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>8.2.1</td>
<td>List of unsupported software prioritised according to business risk, with remediation plan against each item.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>8.2.2</td>
<td>Where it is not possible to upgrade/update software, reasons are given, with associated dependencies.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>8.2.3</td>
<td>The person with overall responsibility for data security confirms that the risks of using unsupported systems are being treated or tolerated.</td>
</tr>
<tr>
<td>8.2 Unsupported software is categorised and documented, and data security risks are identified and managed.</td>
<td>Yes</td>
<td>8.3.1</td>
<td>Provide your strategy for security updates.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>8.3.2</td>
<td>How regularly do you apply security updates to desktop infrastructure.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>8.3.3</td>
<td>How often in days is automatic patching is pushed out to remote endpoints?</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>8.3.4</td>
<td>How many times, in the last twelve months has the SIRO or equivalent senior role been notified where patches have not been applied for longer than two months, with reasons why?</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>8.3.5</td>
<td>List of where updates have not been applied for longer than two months, with reasons why.</td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

Unsupported Platforms: NHS Digital good practice guide

To give real time examples on how to minimise risk levels for unsupported platforms and software.


Obsolete platforms security guidance: National Cyber Security Centre

Short-term steps to take when you can’t move off out-of-date platforms and applications straight away.

https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance#Migrateawayfromobsoletesoftware

Patching guidance for health and care organisations: NHS Digital good practice guide

Guidance on designing and implementing a patching policy to make sure data and systems continue to be properly protected.


Vulnerability management: National Cyber Security Centre

Guidance to help organisations assess and prioritise vulnerabilities.

https://www.ncsc.gov.uk/guidance/vulnerability-management

Care Provider Alliance – Introduction to Cyber Security

Contains helpful hints and tips on improving security and links to additional resources.

https://www.careprovideralliance.org.uk/information-governance.html

Get Safe Online – support for updating software

https://www.getsafeonline.org/protecting-your-computer/
Appendix 3 –

The National Data Guardian Reports

The NDG Report

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’
- the public consultation on that review
- the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care