NHS Digital

Data Security Standard 8

Unsupported systems

The bigger picture and how the standard fits in

2021/22

Information and technology for better health and care

Contents

Overview

The NDG's review data standard 8 states that:

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

Guidance and support is available from NHS Digital to ensure risk owners understand how to prioritise their vulnerabilities. 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.

Using professional judgment

The DSPT guidance (audit framework and associated “big picture guides”) is not exhaustive. They will not cover every eventually and professional judgement will be required in how the standard is met and audited.

Both sets of guidance endeavour to be vendor agnostic. You may have an excellent vendor-supplied system which is not referred to in the guides. That is not to discount such a system, which should be implemented and audited on its merits.

The required standards have to be achievable to those whose digital maturity is still “developing”. As a consequence, some of the measures outlined could be seen as quite manual. This does not mean that more sophisticated measures cannot be implemented.

At times the big picture guides may go further than the audit guides and vice versa. Only the most binary of assertions would lead to one answer. The divergence of guides is either following an implementation theme to the end or the next logical audit artifact

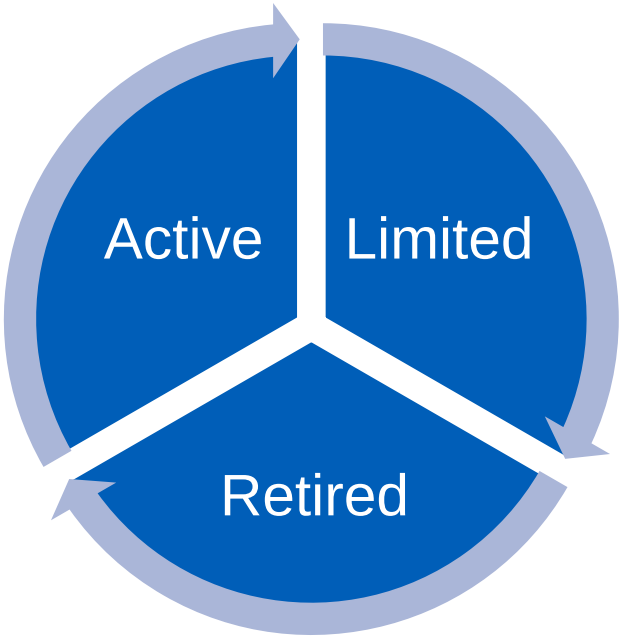
When implementing or auditing please have regard to the intent of the evidence, assertions, standards and ultimately the whole 10 data security standards themselves. It is not the intention of the DSPT to create tick lists of items to be implemented and audited that bear little resemblance to actual practice.

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. Dependent on the manufacturer / type of software, this may be enforced where the old version cannot operate until patched / upgraded

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 no dependencies with a lower risk.

There is no simple rule for all pieces of software, for example, using an operating system from the previous century would pose less of a risk than a recently retired one. As the old operating system is no longer a target for malware, however, due to its vintage it would suffer with connectivity and compatibility issues.



Generally, software will go through three phases:

- active: current product fully supported and patched
- limited: still patched for security though maybe not functionality
- retired: system is unsupported and you should migrate.

Know your IT estate (all of IT)

IT estates

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. The National Data Guardian report discussed using a survey tool can help automate that task.

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 harvest 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 versions of software are those that the manufacturer supports with patching and upgrades. They are 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.

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.

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

Know your boundaries

Understand the boundaries of your IT digital estate and do not overstep them. Know where your network begins and ends, which devices are yours (or you support) and those that are not. Like any good neighbour, liaise with your neighbouring organisations if you are unsure.

Boundaries can occur at many levels, such as multiple network tenancy in a building, between your local network and HSCN, and between wide area networks on the same estate.

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.

Under no circumstances should you scan over HSCN without consulting NHS Digital prior to doing so. Some vulnerability scanners (depending on how aggressively or passively they are being used) can cause a false positive by being indistinguishable from a cyber-attack, with the same tools being used by hackers.

Software cannot exist on its own

Software is installed and used on devices. The devices of interest are end user devices. So that's PCs laptops, tablets and phones. There should be a list of the end user devices used within your organisation (such as a hardware asset database). This can use the same technology as your software assets, as it makes sense to know what software is on what end user device.

You also need to know what removable media assets (such as USB sticks) your organisation has, though it is recognised these can be more difficult to track and control.

Main desktop infrastructure

For most estates, this should be the largest yet the easiest to survey and upgrade, with a standard build, in known and fixed locations, and with desktop PCs managed by the organisation.

However, this can be complicated by:

- no standard build
- no enforced builds
- too wider variety of builds
- staff having local administrator rights.

Provide evidence of how the organisation tracks and records all software assets and their configuration?

Data Security Standard 8.1.1

Does the organisation track and record all end user devices and removeable media assets?

Data Security Standard 8.1.2

Legal and Patched

As well as knowing where your software is you should ensure that you have enough licenses to cover its use. Generally, installed software is licensed per seat or concurrent / pooled licenses.

With a concurrent / pooled license model it is far easier to centrally enforce your license limits. Per seat license can be far more complex with either use of a single shared license / key or unique license per seat.

A shared single license / key, especially one based on trust, can if uncontrolled, easily lead to an organisation exceeding its license threshold. There should be a regular triangulation between your licensing limits and your inventory of software installed on devices.

In keeping to your licensing model means that you should receive security patches (in the active and limited phases) for your software. Those security updates / patches need to be applied in a timely fashion.

Cooperation with other parties

You may not be able to upgrade some of the software on devices yourself i.e. specialist clinical software. Alternatively, software may depend upon certain legacy versions of operating systems or standard software being installed. Examples include an unsupported version of windows or a legacy version of java. It is important that you engage with the supplier of the software and understand the dependencies and any roadmap to compliance.

Where there is no resolution with the supplier, or a fix cannot be applied (due to financial, license or technical reasons), the system should be risk assessed and if appropriate treated as unmanaged and untrusted.

It may be possible to negotiate an extension to a cut-off date, at least in the short term.

There will be systems where updates are no longer available (such as supplier liquidation).

Clinical applications and devices

Care should be taken when surveying and treating clinical applications and devices however they are not exempt or immune to vulnerabilities.

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

See https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices

Remote locations

Where your organisation has remote locations, it will generally fall into one of the categories below:

a) your organisation manages the whole remote site infrastructure including desktops and networking

b) another organisation (such as the main organisation at the remote site) manages the network infrastructure however you still manage the desktops

c) another organisation (such as the main organisation at the remote site) manages the network infrastructure and manages the desktops.

For scenario a) and b), the results of those remote systems should be included in your survey tool results.

For scenario b) and c), you will require cooperation with the other organisation.

Please note, for c) if the other organisation completes the data security and protection toolkit, the survey results can be completed in their submission which means you can just reference it.

Devices and software no longer receiving security updates

The devices and software should either be uninstalled or treated as unmanaged or untrusted (discussed later in this guide).

> Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.
>
> Data Security Standard 8.1.3

> The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.
>
> Data Security Standard 8.1.4

Coverage

Your coverage goal is a minimum 95% of your server estate and 98% of your desktop estate on supported versions of operating systems. This can be determined by Advanced Threat Protection (ATP) or equivalent.

> Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?
>
> Data Security Standard 8.3.7

Managed estates

Where your organisation's complete IT infrastructure is managed by another party, you will require a degree of cooperation with your supplier. Generally, it will be expected that your supplier runs the survey 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

A list from your survey tool (or other method) 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.

> List any unsupported software prioritised according to business risk, with remediation plan against each item.
>
> Data Security Standard 8.2.1

The survey tool (or other method) may be limited by:

- specialist or bespoke applications may not be detected and may require to be manually added
- the survey tool might not be able to detect devices that are on a segmented network.

In both cases, manual intervention may be required to add software or devices to your list.

Risk assessment

Any form of assessment of potential untrusted software should ask the following questions:

1) Is the system built upon components that themselves are subject to vulnerabilities as detailed in cyber alert notifications (formerly CareCERT advisories) that cannot be upgraded or patched?

   Such as requiring an end of life operating system, e.g. an end of life version of Microsoft Server, or built and delivered on a Microsoft SQL Server version that is end of life.

2) Do any of the systems require interaction with components that themselves are subject to vulnerabilities as detailed in cyber alert notifications (formerly CareCERT advisories) that cannot be upgraded or patched?

   Such as a desktop operating system that is end of life or the client requires a legacy version application software.

> The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.
>
> Data Security Standard 8.2.2

If the answer to any of the questions is yes, the system should be treated as an untrusted one and the SIRO should be informed together with mitigation options.

Un-upgradeable devices or software

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

Treat obsolete systems as unmanaged or untrusted

This guide does not go into detail here as there are some great resources (Appendix 2) (Unsupported platforms: NHS Digital good practice guide and Obsolete platforms security guidance: National Cyber Security Centre) that cover this area.

However, one mitigation that has been common is to treat systems as standalone.

The myth of a standalone PC or network

One of the traditional treatments for obsolete systems is to treat them as standalone. In todays connected world, it is difficult to see how a completely standalone system is possible.

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 your network.”
- “It’s that old a piece of software, nobody would ever hack it.”

However, in practice, standalone networks and systems can find themselves directly or indirectly linked to an organisation network.

Direct linking can occur when a device or the network itself is connected temporarily such as to support a data export or installation of new software. This can have the effect of making the entire standalone network vulnerable.

A form of indirect connection can occur with the use of portable drives between the main network and the standalone one which can also make the entire network vulnerable.

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 product 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.

SIRO involvement

The SIRO should be an active role in the process. They need to be informed when systems cannot be upgraded and they should personally confirm what the risks of using unsupported systems are and that these risks are being treated or tolerated.

The SIRO should also be informed where high risk vulnerability patches have not been applied within 14 days, with reasons why. They should also sign off where appropriate on unsupported devices / software

> Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.
>
> Data Security Standard 8.3.4

Have a patching plan

You should have an effective plan or strategy for implementing patches on a consistent and regular basis. You should decide where to use automatic patching (such as the main desktop estate) or where manual patching is more appropriate (such as server farms) and the frequency of that.

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, either through another product such as vulnerability scanner or a dip sample manual check.

You need to decide on how you manage updates to remote end points (Home working PCs or mobile workers). These are devices not on your core network but consume services from the core and which could have a negative effect on the main infrastructure if infected.

How do your systems receive updates and how often?

Data Security Standard 8.3.1

How often, in days, is automatic patching typically being pushed out to remote endpoints?

Data Security Standard 8.3.2

There is a documented approach to applying security updates (patches) agreed by the SIRO.

Data Security Standard 8.3.3

Your patching approach should incorporate a fast track approach for applying critical or high risk vulnerabilities within 14 days of release, though it is recognised that this can be a challenge.

Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.

Data Security Standard 8.3.4

An example patching policy is in Appendix 2: Patching guidance for health and care organisations: NHS Digital good practice guide.

When you can’t patch

Where a decision has been made not to apply a critical or high-risk vulnerability there should be a robust reason for not doing paired with a technical remediation and risk management.

This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.

You should be in a position to know if this a temporary fix such as with a virtual patch on server you intend to patch during the next downtime window or more long term.

Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.

Data Security Standard 8.3.5

Critical Network Infrastructure

Secure by design and configuration

Your infrastructure, ideally when implemented (or retro fitted), should be protected following secure by design principles whether that is network topology or server hardening. This includes ongoing patching and configuration changes.

Secure by design covers having appropriate skill sets, segregation of networks into security zones, simple data flow between components, recoverability and content inspection.

Secure configuration covers knowing your configurable items, utilising baseline and last known good builds managing change, validation, white listing software and managing automated decisions.

Your infrastructure's operating systems and software is patched regularly, the minimum being to the level still supported by the vendor (for security updates).

Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?

Data Security Standard 8.4.1

All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.

Data Security Standard 8.4.2

See

https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-5-resilient-networks-and-systems

Know your exposure

You should manage your infrastructure so you understand its exposure to publicly known vulnerabilities such as NHS Cyber alerts notifications (formerly CareCert) and bodies of knowledge such as Common Vulnerabilities and Exposures cve.mitre.org).

You should prioritise announced vulnerabilities which could be in addition to NHS Cyber alerts notifications (formerly CareCert alerts).

You should test your infrastructure (through 3rd party testing) to verify your understanding.

You should maximise the use of supported software, firmware and networking (i.e. in the active phase).

You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.

Data Security Standard 8.4.3

Appendix 1 -

Table of Data Security and Protection Toolkit Standard 8 Assertions

Assertion	Sub Assertion	Evidence
8.1 All software has been surveyed to understand if it is supported and up to date.	8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration?
	8.1.2	Does the organisation track and record all end user devices and removable media assets?
	8.1.3	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.
	8.1.4	The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.
8.2 Unsupported software is categorised and documented, and data security risks are identified and managed.	8.2.1	List of unsupported software prioritised according to business risk, with remediation plan against each item.
	8.2.2	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.
8.3 Supported systems are kept up-to-date with the	8.3.1	How do your systems receive updates and how often?
	8.3.2	How often in days is automatic patching is pushed out to remote endpoints?

latest security patches.	8.3.3	There is a documented approach to applying security updates (patches) agreed by the SIRO.
	8.3.4	Where a patch for a critical or high-risk vulnerability has not been applied within 14 days, the risk is understood, documented, and has been agreed by the SIRO.
	8.3.5	Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.
	8.3.6	Is your organisation actively using and managing Advanced Threat Protection (ATP)?
	8.3.7	Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?
8.4 You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.	8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?
	8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.
	8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.

Appendix 2 - Useful resources

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

Vulnerability management: National Cyber Security Centre

Guidance to help organisations assess and prioritise vulnerabilities.

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

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