The ITHealth Assurance Dashboard and NHS Digital's Data Security and Protection Toolkit (DSPT)

An NHS mandatory requirement

NHS Digital describes the Data Security and Protection Toolkit (DSPT) as an 'online self-assessment tool that enables NHS organisations to measure and publish their performance against the National Guardian's ten data security standards'. All organisations that have access to NHS patient data and systems must use the toolkit to provide assurance that they are practising good data security and can be trusted with the confidentiality and security of personal information. This document outlines how ITHealth's Assurance Dashboard Solution addresses key requirements of the toolkit, provides supporting evidence and helps maintain ongoing compliance.

ITHealth's Assurance Dashboard Solution consolidates all areas of a Trust's cyber security into a single, near real-time dashboard – giving complete, at-a-glance visibility of the entire network and systems. It increases understanding of a Trust's exposure to risk allowing them to easily report and act upon it, as well as provide the necessary cyber and compliance assurance swiftly and confidently to all key stakeholders. Ultimately, it helps to maintain a secure, vigilant, and resilient IT environment and keeps Trusts justifiably cyber assured at all times.

Achieving and evidencing DSPT compliance

Subject to ongoing development*, the DSPT currently comprises of 44 assertions which break down into a number of evidence items dependant on the category type your NHS organisation falls within. There are four category types within the current DSPT:

- Category 1 - NHS Trusts
- Category 2 - CCGs, CSUs, and ALBs
- Category 3 - Others
- Category 4 - GPs

For the purposes of this document, we refer only to evidence items as specified against Category 1 'NHS Trusts'.

*We also refer to the 2020/21 version of the DSPT (v. 1.1).

Evidence requirements for NHS Trusts (Category 1)

There are a total of 149 evidence items specified for NHS Trusts (Category 1), 110 of which are flagged as 'mandatory'. For an NHS Trust to be deemed 'Satisfactory' it must be able to provide evidence, upon request, for all mandatory evidence items.

Of course, data security includes more than just cyber so the DSPT does encompass other areas; it is, however, the cyber part of the Toolkit that the Assurance Dashboard specifically helps address.

By our deduction, 90 of the 149 evidence items relate to cyber, 68 of which are mandatory. We can, therefore, safely say that **ITHealth's Assurance Dashboard fully meets or supports 81% of the DSPT's cyber-related mandatory requirements** – that's a significant amount for a single solution.

DSPT evidence requirements *met fully* by the ITHealth Assurance Dashboard

The following table details 25 evidence codes, both mandatory and non-mandatory, as listed against category 1 which are fully met by ITHealth's Assurance Dashboard Solution.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps
6.2.2	Number of alerts recorded by the AV tool in the last three months.	Yes	This information is available and can be shown within the Dash-board.
6.2.3	Has anti-virus or malware protection soft-ware been installed on all computers that are connected to or capable of connecting to the Internet?	Yes	The Dashboard shows a full anti-virus status report for all devices and servers. It highlights where anti-virus is enabled, disabled, expired or missing, irrespective of their connectivity.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps
6.2.4	Anti-malware and Anti-Virus is kept continually up to date.	Yes	The Dashboard provides a full anti-virus status report for all devices and servers. Where anti-virus is missing, disabled, or expired, it's possible to schedule and deploy a task from within the Dashboard. These tasks can be set to automatically trigger at the point that anti-virus expires thus removing manual processes.
6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Yes	'Known vulnerabilities' are those listed within CareCERTs and the global CVE database. The Dashboard provides a fully automated CareCERT compliance view. This shows in near real-time your compliance against nearly every CareCERT vulnerability, allowing you to prove that the bulletins and advice are being acted upon. The Dashboard highlights non-compliant assets related to CareCERT alerts and provides an actionable worklist for swifter remediation.
6.3.2	The organisation has responded to high severity CareCERT alerts within 48 hours over the last twelve months.	Yes	The Dashboard ensures the 48-hour response timescale is achievable by taking out much of the manual process of dealing with CareCERTs. Using the Dashboard will also enable Trusts to prove that the 48-hour response timescale has been achieved.
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	Yes	The Dashboard provides a complete software asset inventory and can identify unsupported versions and/or vulnerable configurations.
8.1.2	Does the organisation track and record all end user devices and removeable media assets?	Yes	The Dashboard tracks all assets.
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.	No	The Dashboard provides a complete and current software inventory. Furthermore, the Dashboard provides vulnerability scanning, which will identify unsupported software so the organisation can easily pinpoint unsupported, end of life, or vulnerable versions of software so that, if necessary, these can then be uninstalled.
8.2.1	List of unsupported software prioritised according to business risk, with remediation plan against each item.	Yes	The Dashboard provides a complete, current and accurate hardware and software inventory. This is the cornerstone of assurance strategy. Furthermore, the Dashboard provides vulnerability scanning, which will identify unsupported or vulnerable versions of hardware or software. Vulnerabilities found within publicly available products such as Cisco, Microsoft, Oracle, Java, Adobe, Chrome, etc, will be flagged and ranked according to risk. Remediation of these vulnerabilities can then be tracked via the Dashboard in near real-time resolved. The software products that won't be covered are very bespoke programs, like medical applications. For these, the Trust will need to seek advice from the application vendor as to supported versions. The Dashboard can then be used to verify compliance with what is deployed across the estate.
8.3.1	How do your systems receive updates and how often?	Yes	The Dashboard enables accurate reporting of system updates in near real time.
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Yes	The Dashboard accurately reports on patch status for all assets and includes trends over time.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps...
8.3.3	What is your approach to ensuring patches for critical or high-risk vulnerabilities are applied within 14 days of release?	Yes	The Dashboard reports on all Microsoft patches that have been released and highlights by way of a traffic light report when these patches were applied by the Trust. For example, patches applied within 30 days are highlighted in green, between 30 & 60 days in amber, and then anything over 90 days in red. These timescales can be amended to show uptake within 14 days, if required. Other software status can be reported on. Additionally, ITHealth's technical engineers review the patches that have been applied by the Trust against the Microsoft release to ensure that no patches have been missed.
8.3.5	Is the organisation actively managing Active Threat Prevention (ATP)?	No	The Dashboard provides assurance that ATP is fully deployed and enabled for all components.
8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Yes	The Dashboard will provide assurance as to patching levels across all devices.
8.4.2	All infrastructure is running operating systems and software packages which are patched regularly, and as a minimum in vendor support.	Yes	Operating system and software system patching information is available in the Dashboard, along with supplier information and product details.
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	No	The vulnerability scanning within the Dashboard addresses this.
9.1.1	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed to a high strength password.	Yes	This is discoverable by the Dashboard, so remediation can be carried out for these passwords.
9.3.7	The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service for your publicly visible applications.	Yes	The Dashboard will include the NCSC's Web Check service.
9.4.1	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.	No	The Dashboard is the validation that your security measures are protecting the network and will be able to show if measures are no longer effective as well as what needs to be done to improve protection.
9.4.2	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	No	This is what the Dashboard is designed for - to provide assurance and confidence in the security posture for NHS organisations.
9.4.3	Your confidence in the security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party in the last twelve months.	Yes	The Dashboard provides empirical proof and demonstrates an organisation's compliance, rather than relying on manual systems, spreadsheets, etc. Also, rather than limiting verification to once every 12 months, the Dashboard provides an ongoing 'near real-time' confidence and assurance. ITHealth also provide 3rd party verification.
9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.	Yes	The Dashboard makes it easier for Trusts to prioritise and remediate any security deficiencies.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps...
9.4.6	What level of assurance did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Yes	The Dashboard is a live dashboard 24/7/365 and can therefore verify independently the status of the organisation's assurance levels.
9.6.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and document-ed.	No	The Dashboard captures all assets as they appear on the network, in near real-time. Therefore, any new devices can be flagged. The Dashboard can also be used to document system configurations. The vulnerability scanning service can then be used to ensure that these configurations are secure.
9.7.1	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	Yes	The Dashboard will identify all firewalls.

DSPT evidence requirements *supported* by the ITHealth Assurance Dashboard

The table below details the further 44 evidence codes from the DSPT, both mandatory and non-mandatory, which are supported or met in part by ITHealth's Assurance Dashboard Solution.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps
1.4.2	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	Yes	The Dashboard keeps track of all Trust assets and systems on the network showing asset type, location, and warranty details - making it easier to pinpoint those systems/assets that share personal information.
1.6.2	There are technical controls that prevent infor-mation from being inappropriately copied or downloaded.	Yes	The Dashboard can highlight devices that are vulnerable.
1.6.7	Have any unmitigated risks been identified through the Data Protection Impact Assessment process and notified to the ICO?	No	The Dashboard will show all risks that have been identified.
1.8.1	Does your organisation operate and maintain data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Yes	The Dashboard provides information related to all IT risks, which can feed into the risk register.
1.8.3	What are your top three data security and protec-tion risks?	Yes	The Dashboard is live 24/7/365 so it always provides up-to-date information on the network and at-a-glance visibility of the risks that exist. This ensures that the correct and appropriate infor-mation is always available to facilitate risk-management decision making to identify the top three risks.
2.1.2	When did your organisation last review the list of all systems/information assets holding or sharing personal information?	Yes	The Dashboard provides a list of all systems/assets to support the identification of those that hold or share personal data.
3.3.2	The organisation has appropriately qualified tech-nical cyber security specialist staff and/or service.	Yes	The Dashboard allows non-qualified cyber security specialist staff to have visibility of the Trust's levels of assurance and compli-ance. ITHealth also provide specialist resource.
4.1.1	Your organisation maintains a record of staff and their roles.	Yes	The Dashboard can identify those AD accounts that have no job role assigned. Ensuring these remain accurate once completed will be a manual process.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps...
4.1.2	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Yes	The Dashboard can identify systems and assigned users, plus open shares on the network which aids the identification process.
4.2.1	When was the last audit of user accounts held?	Yes	The Dashboard can identify users within AD and the level of compliance thereby aiding audit purposes.
4.2.2	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	No	The Dashboard can provide supporting information.
4.2.3	Explain how access logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	No	The Dashboard collects a range of logging data related to devices and users and this can be used to review and investigate any malicious activity.
4.2.5	Are unnecessary user accounts removed or disabled?	No	The Dashboard highlights users that haven't logged on to the network for a period of 60 and 90 days. These user lists can be periodically reviewed by the Trust to help determine which user accounts could possibly be removed or disabled.
4.3.2	Are users, systems and where appropriate, devices, always identified and authenticated prior to being provided access to information or systems?	Yes	The Dashboard can provide supporting information.
4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	Yes	The Dashboard can provide supporting information.
4.4.4	The organisation only grants privileged access on devices owned and managed by your organisation.	No	The Dashboard can identify domain and non-domain devices.
4.4.5	You record and store all privileged user sessions for offline analysis and investigation.	No	The Dashboard can record log-in time of privileged access users, as well as device detail and the privileged user credentials. The Dashboard, however, does not record log-out time, so it is not possible to determine the duration of each user session.
4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	No	The Dashboard can identify weak passwords to allow changes to be carried out, password change information is also available.
4.5.3	Multifactor authentication is used [wherever technically feasible].	No	The Dashboard can identify two factor authentication use and also remote session types and usage.
4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high strength.	Yes	The Dashboard can report on password complexity and also on password change frequency.
4.5.6	Do you have high strength passwords defined in policy and enforced technically for all users?	No	The Dashboard can report on password complexity and also on password change frequency.
5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident with findings acted upon.	Yes	The Dashboard provides granular information across all assets allowing investigations to be carried out.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps...
5.1.2	Provide summary details of process reviews held to identify and manage problem processes which cause security breaches.	Yes	The Dashboard provides information across all assets allowing investigations to be carried out to identify problem processes.
6.1.1	A data security and protection breach reporting system is in place.	Yes	The Dashboard is available 24/7/365 and shows all levels of protection and breaches and provides a near real-time reporting system.
6.2.5	Anti-malware (Anti Virus) software scans files automatically upon access.	No	This information is available and can be shown within the Dashboard.
6.2.10	Does the organisation maintain a list of approved applications and are users able to install any application that is unsigned or has an invalid signature?	Yes	The Dashboard can provide a list of approved applications.
6.3.3	The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Yes	The Dashboard will provide monitoring of cyber events alongside systems such as AV, but will also detail those devices that are at risk.
6.3.5	Are all new Digital services that are attractive to cyber criminals for the purposes of fraud, implementing transactional monitoring techniques from the outset?	Yes	The Dashboard provides information relating to applications and services that may be attractive to cyber-crime.
6.3.6	Have you had any repeat data security incidents of the same issue within the organisation?	No	The Dashboard can provide supporting information.
7.1.4	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.	No	The Dashboard provides detailed information about security awareness and threat intelligence which allows changes to be made as required.
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.	No	The Dashboard has an almost real-time view of patching and in addition the monthly assurance reports provided by ITHealth would highlight where patches have not been applied within necessary timescales. The reasons why patches haven't been applied would need to be completed by the Trust.
9.1.2	The Head of IT, or equivalent role confirms all the devices have had their default passwords changed.	No	The Dashboard will identify default passwords.
9.2.1	The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed.	Yes	The Dashboard includes vulnerability scanning of all assets and the identification of default passwords.
9.3.1	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	Yes	The Dashboard will include non-asset vulnerabilities and can provide visibility of websites.

Evidence code	Evidence Text	Mandatory?	How the Assurance Dashboard helps...
9.3.3	The organisation uses the UK Public Sector DNS Service to resolve internet DNS queries.	Yes	The Dashboard includes the ability to check for reference of the UK Public Sector DNS Service.
9.3.5	The organisation understands and records all IP ranges in use across your organisation.	Yes	The Dashboard needs to be aware of all organisational IP ranges and will scan IP based devices.
9.6.1	All devices in your organisation have technical controls which manage the installation of software on the device.	Yes	The Dashboard will identify all software on all devices, as well as related vulnerabilities.
9.6.2	Confirm all data is encrypted at rest on all mobile devices and removeable media and you have the ability to remotely wipe and/or revoke access from an end user device.	Yes	The Dashboard identifies encryption status of all mobile devices. It can identify all removeable media devices to help to determine encryption status.
9.6.4	Only approved software can be installed and run and unnecessary software is removed?	Yes	The Dashboard provides a complete and current software inventory. This facilitates the identification of unnecessary software so that it may be removed.
9.6.5	End user devices are built from a consistent and approved base image.	No	The Dashboard can scan all devices against a gold standard image. Any deviations from this standard are flagged and categorised according to risk level to assist with remediation. This vulnerability scanning ensures that the baseline image can be maintained throughout the Trust.
9.6.6	End user device security settings are managed and deployed centrally.	No	The Dashboard can scan all devices against a gold standard image. Any deviations from this standard are flagged and categorised according to risk level to assist with remediation. This vulnerability scanning ensures that the security settings are managed.
9.6.7	Auto-run is disabled.	No	The Dashboard can report if Auto-run is disabled.
9.6.8	Are proxy servers or equivalent used to provide controlled access to the Internet for relevant machines and users?	Yes	The Dashboard can report if proxy settings are in place.
9.6.10	You have a plan/s for protecting the networked connected IT equipment which you control, which are not connected to the internet or web and application servers, desktop computers, laptop computers, tablets.	No	The Dashboard will identify all assets within the environment and can report whether they are protected or not.
9.7.6	Do all of your desktop PCs and laptops have personal firewalls (or equivalent) enabled and configured to disable (block) unapproved connections by default?	No	The Dashboard can report if a Windows Firewall is enabled.

Ongoing compliance

Submission of the toolkit is required by 31st March annually, with an additional baseline assessment required for larger organisations by the end of October (mainly to indicate that the full assessment is underway). Although only a once a year submission, the toolkit is naturally designed to ensure that the necessary processes and procedures are in place all year round.

The compelling advantage of ITHealth's Assurance Dashboard Solution is that it provides a near real-time view of your IT estate - so you can be aware of your vulnerabilities and compliance levels *at all times*. Any issues and remediation can be addressed in a timely manner ensuring you always remain cyber secure and compliant. In addition, it gives you access to ITHealth's purely NHS focussed technicians who have an unrivalled understanding of NHS IT infrastructures and systems and who provide that third-party witness and verification to the assurance levels of your IT estate.

> "Ultimately, the dashboard acts as an independent witness to everything on the NHIS IT estate. It's this independent view that makes the dashboard so invaluable to us."
>
> MIKE PRESS, Chief Technical Officer, Nottinghamshire Health Informatics Service (NHIS)

> "The level of detail provided within the Dashboard is astounding considering that no agent is needed to be installed on the endpoints."
>
> MIKE HUGHES, Security Specialist, County Durham and Darlington NHS Foundation Trust

> "What I like best is that this system takes away any guesswork and opportunity for error in reporting; it presents a picture of the network and systems as they really are – making it easier to visualise risks and present accurate solutions."
>
> JANET EIVERS, Digital Compliance Manager, Salford Royal NHS Foundation Trust (part of Northern Care Alliance NHS Group)

Stay assured and compliant

Call: 0115 987 6339
Email: info@ithealth.co.uk
Visit: www.ithealth.co.uk/assurance-dashboard

About ITHealth

ITHealth provide NHS organisations with proven and trusted IT security and access management solutions. Whether it's providing fast, reliable, and secure access for NHS mobile workers, or finding effective ways to reduce threats while improving productivity and clinical workflows, ITHealth's cost-effective solutions mean NHS systems and data are always secure, easy to access, and simple to manage.