Ivanti Neurons for Healthcare (powered by Cynerio)

How Healthcare Providers can Comply with Key IoMT Criteria for the NHS Data Security and Protection Toolkit

The National Health Service's (NHS) Data Security and Protection Toolkit (DSPT) is an online self-evaluation that allows healthcare providers in Great Britain to compare their readiness against the National Data Guardian's 10 overarching data security standards. Every organisation that has access to NHS patient data and systems needs to use this toolkit to demonstrate that they have compliant data security for electronic personal health information (ePHI).

British data security standards mandate that healthcare providers ensure that all their devices are protected with no unsupported operating systems or known vulnerabilities present. However, in practice, this is an immensely difficult task to undertake. Connected medical devices come in a huge variety of makes, models and types, each potentially having a custom operating system that often relies on the vendor to support. This is in contrast to a traditional IT security team that typical maintains a handful of well known and supported operating systems.

Medical devices are almost impossible to secure with an agent and it is not uncommon for them to be used well after the vendors have stopped supporting or updating them. However, they continue to play an important role in the environment, often providing critical health services to patients.

Given that hospitals around the world are under tremendous strain from a global pandemic and simultaneously getting hit with an unprecedented barrage of ransomware attacks, it has never been more crucial to identify and remediate the risks that leave medical devices vulnerable to cyber threats.

The NHS broadly agrees with this sentiment. This is why the latest DSPT, set to be made mandatory in June 2022, stipulates that all healthcare providers interfacing with the NHS should have an up-to-date inventory of their medical devices. This inventory should include data about the security posture and any vulnerabilities.

This updated regulation will no doubt force British healthcare providers to view their connected device infrastructure with fresh eyes to make sure they have visibility into all the compliance measures the NHS is now requiring.

At Ivanti, we recommend that healthcare providers be ready for the upcoming DSPT deadline with proactive IoT security that automates risk reduction and visibility across their entire medical device infrastructure. Using Ivanti Neurons for Healthcare (powered by Cynerio) enables healthcare providers to keep their hospitals and clinics secure whilst complying with the NHS directive.

Ivanti Neurons for Healthcare is a leading connected medical device security solution that focuses on addressing the 3 biggest risks facing hospital IoT:

1. **Impacts to patient safety**
2. **Loss of confidential data**
3. **The disruption of patient care and service availability**

For more information on how the Ivanti Neurons for Healthcare can help your organization achieve compliance with the DSPT, see the below table.

DSPT Evidence Item	How Ivanti Neurons for Healthcare (powered by Cynerio) Helps Providers Comply
4.3.2 - Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Ivanti provides detailed, aggregated data about device risks, threats, vulnerabilities, and activity from a wide variety of intelligence feeds, including information from the NHS's own Cyber Alert system. This intelligence can be fed into other IT security platforms such as NACs, firewalls, SIEMs and SOARs through integrations so that any threats can be contained or remediated in real time.
4.5.1 - Do you have a password policy giving staff advice on managing their passwords?	Many medical devices use default passwords or weak credentials, which potentially leaves them and the data they protect vulnerable to exposure. Default passwords are often hardcoded onto the devices, and even if they aren't they usually remain unchanged due to concerns over affecting device warranties or interoperability with other devices. Ivanti allows for the identification of known default or otherwise weak credentials so they can be changed, and leverages service hardening functionality to monitor access to medical devices if passwords are hardcoded onto devices.
4.5.2 - Technical controls enforce password policy and mitigate against password-guessing attacks.	As stated in the section above, Ivanti can identify when a medical device is leveraging a weak, shared or default credential so that it can be replaced by a password that is more complex and much less susceptible to guessing or brute force attacks.
4.5.4 - Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Through Ivanti Neurons for Healthcare, device managers get visibility into vulnerable passwords, such those given to the device by default.
6.3.3 - The organization has a proportionate monitoring solution to detect cyber events on systems and services.	Ivanti monitors the activity of all IoMT, IoT and OT devices that are on a hospital's network. It will identify and alert about any suspicious activity that does not make sense in the pattern of normal device behaviour, and uses threat intelligence feeds with data about known device threats and risks to alert as well, with full reporting on all anomalous activity. This information can also be integrated into IT security response and containment tools to make sure that any threats are quarantined and don't affect patient care or device functionality.

7.1.3 - You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.	Ivanti has an IoMT (Internet of Medical Things) Attack Detection and Response feature for any medical, IoT or OT device a hospital might leverage to treat or care for patients. This gives hospitals the ability to contain and micro-segment device threats by minimizing the types of connections they are allowed to make when a threat is detected on the device. This way, devices can still be safely connected to patients while the device is in use, even if an incident occurs. Ivanti also provides IT and network teams the ability to map the footprint of all IoMT, IoT and OT devices on the network. It includes a virtual segmentation validation engine which can allow these teams to micro-segment devices so that threats on the network are contained to the device where they are located, and even if infection is carried out, the device can still provide normal functionality and patient care.
8.1.1 - Provide evidence of how the organisation tracks and records all software assets and their configuration.	Ivanti passively discovers all IoMT, IoT and OT devices on a network, even when a hospital otherwise has no visibility into their location or characteristics. Ivanti provides automatic identification of every type of device in these categories, including their make, model, brand and over 100 other characteristics and potential risk factors. All of this information is available in drill-down charts down to the individual device level in the portal of the Ivanti platform.
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.	Medical devices and other machines not within the scope of protection by the IT security team often have issues with out-of-date or unpatched operating systems. Ivanti solves this issue by providing the tools for segmenting these devices at the micro level. Proper segmentation can be validated before implementation in the Ivanti portal, where network and IT teams can work together to ensure that segmentation will be secure and won't affect device functionality or patient care. Ultimately this protects medical devices from the risks of a flat network and prevents them from increasing the attack surface should a threat actor gain access to the network.
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.	Ivanti provides hundreds of device remediation plans from within the solution itself for any device risk. In some cases, these will only involve the click of a mouse for resolving the issue across all similar devices on the network. In other cases, it will involve the provision of explicit instructions and links to patches to remediate a device vulnerability. There are also virtual patch options when these patches are unavailable, which will solve the underlying security issue even if the device is not able to technically be patched.

8.2.1 - 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.	Ivanti gives each device on the network a risk score based on a number of different risk factors related to the potential risk to patient safety, service availability or data confidentiality. These risk scores are then organized so that users of the Ivanti portal can clearly see which risks would cause the most problems and must be remediated first, giving hospitals a simple way to prioritize threat mitigation, in addition to complete instructions on how to remediate a threat on each vulnerable device.
8.4.3 - You maintain a current understanding of the exposure of your hardware and software to publicly known vulnerabilities.	Ivanti leverages a number of standard threat and vulnerability feeds as part of its default device intelligence, including those of the NHS and the CVE. Devices with publicly known vulnerabilities can be identified in real time and prioritised by risk level.
9.1.2 - The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	Ivanti allows for the identification and remediation of any IoMT, IoT or OT device with a weak or default password.
9.3.8 - The organisation maintains a register of medical devices connected to its network.	Ivanti passively discovers all IoMT, IoT and OT devices on a network, and provides detailed information about each device including its make, model, brand, serial number and much more. Ivanti can also provide information on current network segmentation, vendor access settings and maintenance arrangements for each device. In addition, Ivanti also goes beyond simple device inventory to provide full risk detection, remediation, and incident response on those devices as well. Finally, Ivanti permits healthcare organizations to validate secure network segmentation across their medical device infrastructure, which cuts down typical network segmentation implementation for connected devices from months to weeks and without disrupting device functionality.
9.3.9 - What is the organisation's data security assurance process for medical devices connected to the network.	Ivanti can collect detailed information on all IoT, IoMT and OT devices on a hospital's network, including detailed data with over 100 characteristics related to each device. Ivanti can tell which devices have access to sensitive electronic personal health information and also prioritises devices based on their risk. Using Ivanti's virtual segmentation engine, the most secure network segmentation architecture can then be applied for these devices on the network, ensuring that their risk exposure is sharply curtailed.

Request a demo to more about how Ivanti can help your healthcare provider comply with DSPT.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Over 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com and follow @GoIvanti.

ivanti neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com