Adopters guidance

Cyber security and resilience for health or care services

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Medicines and Healthcare products Regulatory Agency (MHRA)
- Department for Health and Social Care

Last updated: 18 April 2024

Cyber security is the protection of devices, services and networks and the information on them from theft or damage. It's essential for providing effective care, protecting patient and service user safety and maintaining trust in your service.

The Network and Information Systems Regulations

The Network and Information Systems Regulations 2018 aim to improve cyber security. Network and information systems (NIS) include:

- electronic communications networks
- devices or groups of interconnected devices that automatically process digital data, and
- digital data stored, processed, retrieved or transmitted by either of the above for the purposes of their operation, use, protection and maintenance

The regulations place security and reporting duties on an operator of essential services (OES). Healthcare services are an essential service under the regulations. The OESs in England are:

- NHS trusts or foundation trusts
- integrated care boards
- certain independent providers of healthcare

The regulations require an OES to:

- take appropriate and proportionate technical and operational measures to
- manage risks posed to the security of the NIS on which its essential service relies
- minimise the impact of incidents affecting the security of the NIS used for the provision of its essential services
- report any incident that has an adverse effect on the security of the NIS and a significant impact on the continuity of the essential service, within 72 hours. Your organisation should do this using the Data Security and Protection Toolkit (DSPT)

These duties also apply where there are physical and environmental causes such as interruptions to power supply or flooding.

Enforcing the NIS Regulations

The Secretary of State for Health and Social Care is the competent authority (regulator) acting through the Department of Health and Social Care. They are responsible for overseeing the NIS Regulations for healthcare services in England.

Under the NIS Regulations, the Secretary of State for Health and Social Care has powers to:

- issue an information notice requiring an OES to provide information
- do an inspection
- issue an enforcement notice requiring action to address failings
- issue a penalty notice for a financial penalty up to £17 million

Data Security and Protection Toolkit

The DSPT is NHS England's online self-assessment tool for data security and protection requirements. It includes the NIS Regulations. If your organisation has access to NHS patient data and systems, you must use the toolkit to show you're practising good data security and that personal information is handled correctly.

Your organisation should complete and publish a DSPT assessment in accordance with the DAPB0086: Data Security and Protection Toolkit information standard published under section 250 of the Health and Social Care Act 2012.

Cyber Essentials

Cyber Essentials is a self-assessment certification that helps you protect your organisation against cyber attack. It helps you guard against the most common cyber threats and demonstrates your commitment to cyber security.

You may use Cyber Essentials to meet contractual obligations with other organisations, such as insurance providers or suppliers. Some contracts require Cyber Essentials or a higher level of certification (Cyber Essentials Plus). Organisations with Cyber Essentials Plus certification do not have to respond to some DSPT questions. But Cyber Essentials Plus certification is not required for completing the DSPT.

The government also requires suppliers bidding for certain types of public contracts (for example those where personal data of citizens, such as home addresses, is handled by

suppliers) to hold Cyber Essentials or Cyber Essentials Plus certification (or demonstrate that equivalent controls are in place).

The Cyber Assessment Framework

The National Cyber Security Centre's Cyber Assessment Framework is a tool for assessing cyber resilience (the extent to which cyber risks to essential functions are being managed by your organisation). It is widely used across other sectors and will be rolled out for health and care as updates to the established DSPT process. The framework establishes cybersecurity outcomes without defining how they should be met, empowering your organisation to manage its risk proportionately and with autonomy. Further information on implementation timelines for your organisation will be published on the DSPT website.

Digital Technology Assessment Criteria

The Digital Technology Assessment Criteria (DTAC) include cybersecurity requirements for digital technologies used in health or social care. You can assess a developer's completed DTAC during procurement or as part of a due diligence process, to make sure the digital technology meets minimum cybersecurity standards.

Medical devices

Digital healthcare technologies classified as medical devices are regulated by the Medicines and Healthcare products Regulatory Agency (MHRA). It has published a plan to address cybersecurity issues for medical devices - see it's cyber secure medical devices work package for more information.

You should report safety concerns about medical devices to the MHRA using its Yellow Card scheme or via the Yellow Card app.

Further reading

- The Network and Information Systems Regulations: guide for the health sector in England on GOV.UK
- Cyber security strategy for health and social care: 2023 to 2030 on GOV.UK
- National Cyber Security Centre: advice and guidance

