Developers guidance

Cyber security and resilience for digital healthcare technologies

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Information Commissioner's Office (ICO)
- 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 services.

The Network and Information Systems Regulations

The Network and Information Systems (NIS) Regulations 2018 place security and reporting duties on relevant digital service providers (RDSPs).

RDSPs are organisations that provide specific types of digital services:

- online search engines
- online marketplaces
- cloud computing services

To be an RDSP you must provide one or more of these services, have your head office in the UK or provide digital services within the UK (where your head office is outside of the UK, in which case you must nominate a representative in the UK).

Small and micro organisations are exempt. If you have fewer than 50 staff and an annual turnover or balance sheet below €10 million then you are not an RDSP, and the NIS Regulations do not apply. But if you are part of a larger group, you should assess the group's staffing and turnover numbers to see if the exemption applies.

RDSPs are required to register with the Information Commissioner's Office (ICO). This is the competent authority (regulator) for RDSPs. Under the NIS Regulations, the ICO has powers to:

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

Reporting incidents to the ICO

Under the NIS Regulations, RDSPs are required to notify the ICO of any incident that has a substantial impact on the provision of their services. You must notify the ICO without undue delay and no later than 72 hours. You can assess whether you need to notify and report an incident using the ICO's incident reporting guide. You should also consider notifying the National Cyber Security Centre at the same time.

Personal data breaches

Under the UK General Data Protection Regulation, incidents that result in a personal data breach must be reported to the ICO. See how to comply with the UK GDPR for more information.

Adverse incidents for medical devices

If your technology is a medical device, you must report any adverse incidents to the Medicines and Healthcare products Regulatory Agency using its MORE portal. For more information, see post-market surveillance of medical devices and identifying adverse incidents for software as a medical device.

Data Security and Protection Toolkit (DSPT)

The DSPT is NHS England's online self-assessment tool for data security and protection requirements. 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. The government 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). 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 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

If you want your technology to be used in the NHS or social care, you may be asked to demonstrate that it meets the standards set by the Digital Technology Assessment Criteria (DTAC). These include cybersecurity requirements. During procurement, adopters will review your completed DTAC to make sure your technology meets minimum standards.

Further reading

- ICO: The Guide to NIS
- Cyber security strategy for health and social care: 2023 to 2030 on GOV.UK
- National Cyber Security Centre: advice and guidance

