Department of Health & Social Care

The Network and Information Systems Regulations 2018

Guide for the health sector in England

May 2018

DH ID box
Title: The Network and Information Systems Regulations 2018: Guide for the health sector in England
Author: DDP/ Cyber Security / 13920
Document Purpose: Policy
Publication date: May 2018
Target audience: NHS providers
Contact details: See page 8

Published to gov.uk, in PDF format only.

www.gov.uk/dh

Overview

The Network and Information Systems Regulations 2018 (NIS Regulations) place security and reporting requirements on ‘operators of essential services’. Where operators do not comply with these requirements regulatory action, including penalties of up to £17 million, can be taken.

For the health sector in England NHS healthcare is considered an essential service. Accordingly, NHS Trusts and Foundation Trusts are designated as ‘operators of essential services’ along with other organisations who will be individually notified. The Department of Health and Social Care will be responsible for overseeing the operation of the NIS Regulations within the sector.

To ensure a joined up approach to implementation the NIS Regulations have been incorporated into our wider approach to implementing the National Data Guardian’s 10 data security standards. These data security standards apply to all health and care organisations to ensure that systems and data are protected.

While the NIS Regulations will only apply to organisations in scope, the 10 data security standards and wider regulatory framework, including the General Data Protection Regulation (GDPR), apply to all health and care organisations.

Contents

Background

The NIS Regulations seek to ensure that 'essential services' in member states, including health, have adequate data and cyber security measures in place. It applies to those sectors which are vital for our economy and society, providing services such as healthcare, transport and the supply of electricity and water.

The Regulations require organisations identified as 'operators of essential services' to take appropriate and proportionate measures to:

- manage risks posed to the security of the network and information systems on which their essential services rely;
- prevent and minimise the impact of incidents on the delivery of essential services; and
- report serious network and information incidents that impact on provision of the essential service.

This will be overseen by 'competent authorities' which will fulfil a similar role to a regulator, with the power to issue guidance, inspect organisations and take enforcement action (including penalties of up to £17 million) where necessary.

Application to the health sector in England

The health sector is one of six economic sectors considered "essential" under the NIS Regulations. In England NHS healthcare is an essential service for the purposes of the NIS Regulations. Only organisations that can significantly disrupt the delivery of essential services are considered 'operators of essential services' under the NIS Regulations.

As such NHS Trusts and Foundation Trusts are considered 'operators of essential services' for the health sector in England for the purposes of the NIS Regulations. The Department will also designate other NHS healthcare providers as 'operators of essential services' and those organisations will be individually notified.

The Department of Health and Social Care will be responsible for overseeing the operation of the NIS Regulations within the sector. This includes taking enforcement action where necessary. NHS Digital will produce guidance for operators, and provide technical support to the Department.

The National Cyber Security Centre (NCSC) are the national technical authority under the NIS Regulations, and are therefore responsible for supporting operators of essential services and the competent authorities by publishing guidance[1] and acting as a source of technical expertise.

[1] https://www.ncsc.gov.uk/guidance/nis-guidance-collection

Complying with the NIS Regulations

Fulfilling the security duties

The Department's approach is to as far as possible integrate the implementation of the Regulations into the existing data and cyber security programme and align it with existing tools and mechanisms, using the Regulations to support the aims of that programme. Providers who are designated operators of essential services will therefore be expected to fulfil the security duties of the NIS Regulations through implementing the National Data Guardian's 10 data security standards. NHS Digital will publish guidance on implementing the 10 data security standards, incorporating the requirements for fulfilling the security duties of the NIS Regulations. This guidance will be accessible through the Data Security and Protection Toolkit ("the toolkit")[2], and will be updated over time and reflect relevant guidance from NCSC.

While not all health and care organisations will come within scope of the NIS Regulations, all are held to the same high standard that reflects the sensitivity of data and criticality of systems in health and care. All health and care organisations must comply with the National Data Guardian's 10 data security standards and the General Data Protection Regulation.

Incident reporting

The incident reporting tool in the toolkit is intended to fulfil legislative reporting requirements for NIS incidents and GDPR breaches**. For support with data security incident response you can contact NHS Digital via the Data Security Helpline (0300 3035 222)**. Where appropriate, NHS Digital will work with NCSC to manage and resolve incidents.

Under the NIS Regulations, operators of essential services are required to report any network and information systems incident which has a 'significant impact' on the continuity of the essential service that they provide. This must be done without undue delay, and in any event within 72 hours of becoming aware of the incident. NHS Digital will make detailed guidance available through the toolkit on incident reporting under both the NIS Regulations and GDPR, which will explain when an incident is considered to have a 'significant impact' under the NIS Regulations.

All health and care organisations, regardless of whether they are in scope of the NIS Regulations, are required to report GDPR breaches through the toolkit. This includes breaches relating to network and information systems. A network and information systems incident that disrupts the delivery of health and care, or compromises the confidentiality of health and care data, is likely to risk the rights and freedoms of individuals. Therefore such incidents should be reported through the toolkit in line with GDPR requirements even where there is not a requirement to report the incident under the NIS Regulations.

[2] https://www.dsptoolkit.nhs.uk

Oversight

Monitoring Compliance

The Department of Health and Social Care is responsible for overseeing the operation of the NIS Regulations in the health sector in England. The Department will do this by using information collected by NHS Digital, including through the toolkit and onsite assessments.

To demonstrate their fulfilment of the security duties of the NIS Regulations, operators will be required to complete the toolkit (like all health and care organisations) and undergo onsite assessments arranged by NHS Digital as part of the existing onsite assessment programme.

All health and care organisations are required to complete the toolkit to demonstrate their compliance with the relevant data security and data protection requirements. The toolkit incorporates a broad range of data security and data protection requirements, including the National Data Guardian's 10 data security standards, the NIS security duties and GDPR. Over time the required assertions and evidence items in the toolkit will be updated to increase alignment with relevant guidance from NCSC.

Inspections

Under the NIS Regulations the Department of Health and Social Care has the power to inspect operators. However, the Department intends to rely on information collected by NHS Digital to monitor compliance with the NIS Regulations. This includes information collected through the toolkit and onsite assessments. Therefore, it is the Department's policy to only use its power to inspect where NHS Digital is unable to obtain sufficient information or in response to a specific concern.

Enforcement

Where operators do not comply with the NIS security duties, the Department has the power to take regulatory action including:

- Issuing an Information Notice to request information;
- Issuing an Enforcement Notice to require action to address failings; and
- Issuing a Penalty Notice levying a financial penalty not exceeding £17 million.

While any enforcement action will be proportionate, the Department intends to use its full range of enforcement powers where sufficient action is not being taken by operators.

Right to an independent review

Operators of essential services will have the right to request an independent review of a decision to designate them as an operator (on a case by case basis), or issue a Penalty Notice to them. The Department will appoint an independent person to make decisions on appeals. Further information will be provided should an organisation request an independent review of a designation or penalty decision.

Contact

- For support with data security incident response you can contact NHS Digital via the Data Security Helpline (0300 3035 222).
- To formally report incidents under the regulations please use toolkit: https://www.dsptoolkit.nhs.uk .
- For general information about data security and fulfilling security duties please contact NHS Digital at enquiries@nhsdigital.nhs.uk.
- For questions about the application of the regulations or this guide please contact NIS.Authority@dh.gsi.gov.uk.