NHS England

Data Security Standard 10

Accountable suppliers

The bigger picture and how the standard fits in

2023/24

Information and technology for better health and care

Contents

Overview

The National Data Guardian's (NDG) Data Security Standard 10 - Accountable suppliers, states the following:

"IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards."

IT suppliers understand their obligations as data processors under the UK General Data Protection Regulation (UK GDPR), and the necessity to educate and inform customers, working with them to combine security and usability in systems.

IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course.

It's the responsibility of suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plugins.

Please refer to further note on professional judgement, auditing and UK GDPR.

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/using-professional-judgement

Your suppliers and contracts (10.1.1 – 10.3.1)

List your suppliers (10.1.1)

You should know which contracts you have in place with suppliers that handle personal data, and suppliers that provide IT services. This will include, for example, catering services if they handle personal data that includes patient names and dietary requirements, and suppliers that may not be primarily IT-based, but whose service includes an IT component.

Depending on the size of your organisation, this may be a trivial or a more complex task. For example, asking a GP to list systems supplier details should be relatively easy, whereas a multi-site large provider with a wide breadth of services combined with a decentralised procurement would be more challenging.

Any form of surveying and scanning activities to survey your systems (as referenced in NDG Data Security Standard 8) may yield an unacknowledged system(s) and new supplier(s).

The information that should be recorded is the products and services they deliver, their contact details and the contract duration, as in the example below:

Supplier	Products	Services	Cert	Contract	Start and end date
AA1 Clinical IT System	AA1-Pas AA1-Pathology AA1-Radiology	In addition to supply of systems, on site support and remote diagnosis and extracts	CE+	\\sharepoint\contract\IT\AA1	dd/mm/yy – dd/mm/yy
eRoster	eRoster Pro	Web based staff rostering system	ISO 27001	\\sharepoint\contract\IT\eRester	dd/mm/yy – dd/mm/yy
No Laughing Matter Ltd	Medi Gas Safe	Nitrous oxide and entonox staff levels monitoring	No	\\sharepoint\contract\IT\nolaugh	dd/mm/yy – dd/mm/yy

		service with web portal			
Citizen Services	Remember you're a member RYAM 2.2	Membership registration and my membership portal.	CE+	\\sharepoint\contract\IT\RYAM	dd/mm/yy – dd/mm/yy

Your organisations may also have contracts with payroll or HR services, suppliers of software platforms such as for remote monitoring or mood tracking, laboratory testing of samples amongst others. This list is not exhaustive, and you should consider all contracts you have that may have a data protection or security impact.

Under the UK General Data Protection Regulation (UK GDPR), you will have data controller responsibility and be expected to know and provide direction to your suppliers

Supply chains with an IT element

When it comes to identifying suppliers, it is easy to identify those whose primary business and contract relate to IT systems.

However, not every contract is readily identifiable as having an IT systems component. For example, a supplier who monitors gas levels for staff safety may have an IT systems component bundled into their wider service offering, or may subcontract the IT systems element from a secondary supplier.

There is no simple answer way of deducing where all IT systems containing personal data do and do not exist, but with increasing digitisation, it is safer to assume that any sizeable contract will have an IT system that may contain personal confidential data.

"Knowing your suppliers well is vitally important."

Darren Mort, NHS England

Cloud supplier

Any sizeable cloud contract will invariably mean moving some personal confidential data into the cloud.

A cloud contract with storage containing personal confidential data should be included as a system.

Guidance on implementing cloud services in health and care

NHS and social care data: off-shoring and the use of public cloud services

National guidance for health and care organisations who want to use cloud services or data offshoring to store patient information.

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services

Contracts

If you are a controller appointing a processor, you must have a legally binding agreement in place when processing personal data. This could be a contract or a data processing agreement. A service level agreement or accepting an app's terms and conditions are examples of a contract. If you are using a contract that doesn't have a section on data protection, you must also have a data processing agreement.

Any contract or agreement must have the appropriate clauses in place to cover the requirements of data protection legislation. Article 28 of UK GDPR sets out the requirements when appointing a processor.

The NHS standard contract contains all of the necessary clauses needed to comply with UK GDPR and should be used where possible. You just need to fill in schedule 6F of the NHS standard contract with the details of the processing.

If you are not using the NHS standard contract, the following checklist provides a guide to the necessary clauses for any legally binding agreement between a controller and a processor. Depending on the agreement involved, these clauses may be captured within the body of the main contract, as a separate schedule, or as a standalone data processing agreement.

Organisations are responsible for seeking their own legal advice and ensuring any contracts they sign are fit for purpose.

General clauses in the agreement

Confidential information has been defined as both personal data and sensitive corporate and commercial information.

Requirements that the processor will:

- only act upon direct instruction from the controller (unless there is a legal requirement to provide data e.g. a court order)
- ensure the same or higher requirements are placed on any sub-processor, with associated processing restricted to that agreed to in the agreement or further written instructions from the controller
- not engage further sub-processors beyond those set out in the contract without the written agreement of the controller
- maintain the confidentiality of confidential information, which extends beyond the expiry of the agreement

- ensure staff have been appropriately trained and are contractually bound to keep data confidential
- report any data breach immediately to the controller and detail the data affected with approximate number of data subjects implicated, the categories of data, the nature of the breach and any measures taken to mitigate it
- hold a written record of processing activities and will provide a copy on demand
- allow auditing of their processing
- guarantee that it has implemented sufficient organisational and technical measures to safeguard the data (including DSPT and other relevant requirements) and that measures are regularly tested for resilience
- ensure business continuity measures are in place and monitored
- cooperate with other parties, particularly in relation to: completion of data protection impact assessments (DPIAs), assisting the controller to fulfil their duties with regard to information rights requests
- indemnify the controller for any Information Commissioner's Office (ICO) action or fines for any area where the processor has been found to be negligent or responsible

Specific in the agreement

Details of the agreed processing to be undertaken, restricted to what is detailed within the agreement unless the controller's written agreement has been obtained including:

- categories and types of data
- categories of data subject
- purpose of processing
- legal basis under UK GDPR
- level of identifiability (identifiable, anonymous, pseudonymised)
- security arrangements for data in transfer and data at rest
- permitted geographical location and whether data is transferred outside the UK. See 'What should be used where data is transferred outside the UK?'
- a list of any sub-processors
- details of what happens if the processor comes under new ownership, goes out of business or is under administration, with particular regard to the data it holds
- clearly defined responsibilities under Freedom of Information Act 2000, Environment Information Regulations 2004, and data protection legislation
- details of what will happen to the data at termination of the agreement (secure destruction with certificates, or transfer of the data to another organisation, along with the methods
- a clearly defined dispute resolution process
- commencement and expiry date

- details of the Processor's Data Protection Officer (where applicable)
- authorised signatories and the agreement has been signed

What should be used where data is transferred outside the UK?

The UK has 'adequacy regulations' for a number of countries that have been assessed as providing adequate protection for individuals' rights and freedoms in relation to their personal data. You should document where the data is flowing to within your contract and ROPA.

Commented [TG1]: Suggest changing link to UK approach to international data transfers - GOV.UK (www.gov.uk)

The document currently linked is a PDF file which will be taken down at some point

Commented [MD(EX2R1]: accepted

Where data is transferred to a country with no adequacy regulation, known as a 'third country' the ICO recommends that you should use the International Data Transfer Agreement (IDTA) template. Where you have standard contractual clauses already in place to cover the data transfer, you should also complete the IDTA Addendum before 21 March 2024. You can reference the IDTA documents within other agreements (such as the NHS standard contract) if needed. You can also use derogations or binding corporate rules, but the application within health and care may be more complex or less relevant

Due diligence (10.2.1)

Prior to awarding a contract

Due diligence involves researching candidate organisations so that you can be assured of their compliance with data protection laws and the NDG Data Security Standards.

This includes checking their DSPT status for the latest year's submission, and if you are contracting suppliers to provide digital health and care technology, you are encouraged to request and review their Digital Technology Assessment Criteria (DTAC) submission.

It is important to note that the level of due diligence needed will depend on the level of risk of the service the supplier is providing, as well as your organisation's appetite for risk. However, if an organisation is commissioned via the NHS Standard Contract, the Provider must complete and publish an annual information governance assessment in accordance with in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider's organisation type. (21.2 General Responsibilities).

Supplier Certification

An organisation should ensure that any supplier of critical IT systems that could impact on the delivery of care, or that processes personal identifiable data, has the appropriate certification (suppliers may include other health and care organisations).

Depending on the nature and criticality of the service provided, certification might include:

- ISO/IEC 27001:2013 certification: supplier holds a current ISO/IEC27001:2013 certificate issued by a United Kingdom Accreditation Service (UKAS) - accredited certifying body and scoped to include all core activities required to support delivery of services to the organisation
- Cyber Essentials (CE) certification: supplier holds a current CE certificate from an accredited CE certification body
- Cyber Essentials Plus (CE+) certification: supplier holds a current CE+ certificate from an accredited CE+ Certification Body
- Digital Marketplace: supplier services are available through the UK Government Digital Marketplace under a current framework agreement
- Other types of certification may also be applicable. Please refer to Cyber Security Services 2 Framework via Crown Commercial.

NHS England contracts for/supplies a number of IT systems and solutions in use by multiple NHS organisations.

Please note that NHS England ensures in each of its system procurements that appropriate data security certifications are in place from its suppliers.

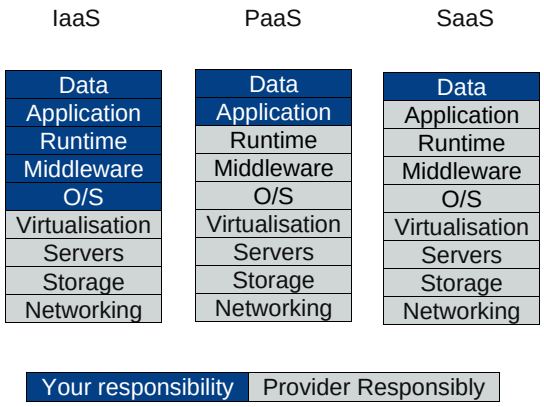
However, it is important that your organisation assures itself of any necessary certification for suppliers it uses, even if the procurement has been done through a framework.

Outsourced responsibility (10.2.4)

Services such as cloud computing solutions are a good example of there being shared responsibilities for support between the customer and provider.

There are 3 cloud models with varying levels of responsibility between you and your provider:

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)



Further information on each of the models is given in the National Cyber Security Centre's guidance.

It is important to know where your responsibilities end and your providers' begin to ensure nothing falls between the gaps and responsibilities are clearly outlined and documented in your contracts.

National Cyber Security Centre cloud security guidance

How to configure, deploy and use cloud services securely
The 3 models are discussed here

https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/technically-enforced-separation-in-the-cloud

In execution there will differences in how cloud suppliers deliver their models, for example Amazon's AWS Shared Responsibility Model.

This means you must know contract by contract who is responsible for what security maintenance. It should be noted that although you can outsource responsibility you always retain accountability as a data controller.

Suppliers / data processors / joint controllers completing a toolkit (10.2.5)

Every supplier, data processor and joint controller linked to your organisation who processes personal or confidential information must have completed a data security and protection toolkit. It is your responsibility to check that they have done so. If not, they should be able to demonstrate an equal or higher standard.

Please be advised that merely viewing personal or confidential information is still classified as processing.

Suppliers completing the Data Security and Protection Toolkit (DSPT) can self-assert that they reached the data security standard. This allows a level playing field to a known standard.

Managing supplier incidents (10.3.1)

As well as the usual business contract monitoring process, any incidents/nonconformities to the NDG standards that have a data security or data protection implication, should be recorded.

These include incidents as well as near misses.

The vast majority of incidents from processors will be reported without undue delay to the controller. However, remember that under UK GDPR, processors can report incidents independently, including ones concerning the data controller.

An example of a list of disputes with supplier/controllers is shown below.

Supplier	Products	Incident	Escalation	Start and end date
AA1 Clinical IT System	AA1-Pas	Supplier won't encrypt its primary patient index. Although other modules are encrypted.	Escalated to supplier via account director. dd/mm/yy	dd/mm/yy – dd/mm/yy
eRoster	eRoster Pro	The rostering templates for another organisation (with different start / end times) was applied to our organisation causing confusion and problems at changeover. May have contributed to clinical care.	Not a data loss but logged on DSPT Incident as well as STEIS and subject to a full audit and outcomes.	dd/mm/yy – dd/mm/yy
No Laughing Matter Ltd	Medi Gas Safe	During an upgrade, the UK datacentre moved the application on a temporary VR instance which was hacked and data exfiltrated containing staff medical information.	Logged on Incident tool on DSPT reportable to ICO and under investigation.	dd/mm/yy – dd/mm/yy
Citizen Services	Remember you're a member RYAM 2.2	Members complained of increased target phishing mails referencing their membership. Supplier denies any incident has occurred.	Under investigation dd/mm/yy	dd/mm/yy – dd/mm/yy

Non-compliance with NDG Data Security Standards due to supplier / processor issues (10.4.1)

Where your organisation is unable to comply with the NDG Data Security Standards due to a supplier or processor issue (not a local issue), this should be recorded.

The types of issues could be:

- a clinical system needs to run on an unsupported/retired operating system or application, thus consequently endpoints cannot be patched
- supplier refusing to conduct/be involved in continuity planning
- supplier unable to verify staff training in data protection/security
- supplier not reporting incidents
- processor retains sensitive records longer than the records scheduled retention date due to technical referencing reasons
- a supplier not fixing OWASP Top 10 issues for a supplier-maintained web site
- a supplier unable to demonstrate compliance with data protection legislation
- a supplier not acting upon CareCert advisories
- a supplier who should but is unwilling/unable to complete the Data Security and Protection toolkit

This should be recorded as per the example on the previous page and discussed at board level (if a pure supplier issue).

Risk

Traditionally organisations have treated risk management as being within its organisational boundaries. You had your risk and supplier had theirs.

However, suppliers can have an effect on the delivery of your services which in turn can affect individuals' rights and freedoms. Therefore, you must extend your risk management process to those suppliers involved in the networks and information systems. This can either be viewed as a supply chain issue or an issue for processing data under UK GDPR. Regardless, your risk management processes must take into account risks on your suppliers' end.

You should be aware of your risk exposure in terms of outsourcing your systems to external suppliers. For example, an organisation with the same supplier for all its clinical and financial systems would experience a more significant impact with a supplier outage than an organisation with multiple suppliers.

Mutual support (10.5.1)

Given the interdependencies with your supplier, assisting them (where appropriate) to resolve an incident can be mutually beneficial.

Appendix 1 - Useful resources

Supply chain security guidance: NCSC - A series of 12 principles, designed to help you establish effective control and oversight of your supply chain.
https://www.ncsc.gov.uk/collection/supply-chain-security

Guide to UK GDPR accountability and governance contracts: ICO - The ICO's guide to written contracts between controllers and processors.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

UK GDPR guidance contracts and liabilities between controllers and processors: ICO – The ICO's overview of contracts as a legal basis for processing.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/

UK GDPR Regulations: The European Parliament and the Council of the European Union - On the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

UK GDPR checklist: ICO - Checklists to assess compliance with data protection law and find out what you need to do to make sure you are keeping people's personal data secure.
https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/

Appendix 2 – Data security reports

The National Data Guardian review

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

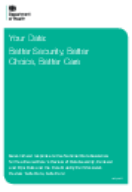
The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’;
- the public consultation on that review;
- the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.



Your Data: Better Security, Better Choice, Better Care