NHS Digital

Data Security Standard 10

Accountable suppliers

The bigger picture and how the standard fits in

2021/22

Information and technology for better health and care

Contents

Overview

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

"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 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 is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

Using professional judgment

The DSPT guidance (audit framework and associated “big picture guides”) is not exhaustive. They will not cover every eventually and professional judgement will be required in how the standard is met and audited.

Both sets of guidance endeavour to be vendor agnostic. You may have an excellent vendor-supplied system which is not referred to in the guides. That is not to discount such a system, which should be implemented and audited on its merits.

The required standards have to be achievable to those whose digital maturity is still “developing”. As a consequence, some of the measures outlined could be seen as quite manual. This does not mean that more sophisticated measures cannot be implemented.

At times the big picture guides may go further than the audit guides and vice versa. Only the most binary of assertions would lead to one answer. The divergence of guides is either following an implementation theme to the end or the next logical audit artifact

When implementing or auditing please have regard to the intent of the evidence, assertions, standards and ultimately the whole 10 data security standards themselves. It is not the intention of the DSPT to create tick lists of items to be implemented and audited that bear little resemblance to actual practice.

Know your suppliers

List them

You should know your suppliers of IT which handle personal information, IT services and the contract with suppliers, which may not be primarily IT based but have an IT element.

Dependent on the type of 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 2) 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 service with web portal	No	\\sharepoint\contract\IT\nolaugh	dd/mm/yy – dd/mm/yy
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

The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.

Data Security Standard 10.1.1

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

Supply chains

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 and a supplier may subcontract for the IT systems element.

Looking at our example of the monitoring gas levels for staff safety, it is the type of service that may be bundled into a wider service offering or subcontracted by the primary supplier.

"Knowing your suppliers well is vitally important."

Darren Mort, NHS Digital

Consequently, it may not be that clear to those responsible for gathering supplier information that there is an IT systems element; for example, a radiology service contract where a subcontractor services and maintains medical devices which contain patient confidential data.

There is no simple answer, but with increasing digitisation, it is safer to assume that any sizeable contract will have an IT system within it that may contain personal confidential data.

Cloud supplier

Any sizeable cloud contract will invariably mean moving some personal confidential data into the cloud. Cloud contract with storage containing personal confidential data should be included as a system.

For guidance on implementing cloud services in health and care see

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

As well as knowing their nature and length, contracts should be reviewed to ensure GDPR compliance as stated in Article 28 of the GDPR. Under Article 28, controllers must only appoint processors who can provide “sufficient guarantees” to meet the requirements of the GDPR.

Many of the contractual obligations necessary to comply with GDPR and the Data Protection Act 2018 were already required under the Data Protection Act (DPA 1998) 1998 and/or NHS Standard Contracts - key components are set out in NDG Data Security Standard 1: Personal confidential data.

The GDPR introduces some key changes that must be incorporated within third party contracts to reflect the new obligations placed on data processors by Article 28. For example:

- the data processor’s liabilities in respect of a breach of GDPR;
- the data processor’s liability for a breach by one of their sub-contractors.

You should consider how you will:

- review third party contracts;
- update contracts to reflect new responsibilities;
- address non-compliance by your third party contractors.

The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA 1998.

These contracts must now include certain specific terms, as a minimum.

These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).

The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

When is a contract needed?

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller), it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

What needs to be included in the contract?

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- notify the controller without undue delay if it becomes aware of a breach of the personal data it is processing on behalf of the controller;
- delete or return all personal data to the controller as requested at the end of the contract; and

- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the

controller immediately if it is asked to do something that would infringe the GDPR or other data protection law of the EU or a member state.

Can standard contracts clauses be used?

The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (in the UK, the Information Commissioner's Office) to be used in contracts between controllers and processors.

The Commission plans to update the existing standard contractual clauses for the GDPR. Until then, you can still enter into contracts which include the Directive-based standard contractual clauses. Please keep checking the websites of the ICO and the Commission for further information.

If you are entering into a new contract, you must use the standard contractual clauses in their entirety and without amendment. You can include additional clauses on business related issues, provided that they do not contradict the standard contractual clauses. You can also add parties (i.e. additional data importers or exporters) provided they are also bound by the standard contractual clauses.

See

https://ico.org.uk/for-organisations/data-protection-and-brexit/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/

The GDPR also allows these standard contractual clauses to form part of a code of conduct or certification mechanism to demonstrate compliant processing. However, no schemes are currently available.

Where suppliers hold personal data on your behalf and they act as processors, they may only process the data in accordance with your written instructions. This means that legally the processor must not disclose information to anyone else unless they have told you about the request beforehand and you have told them to comply with it (**you should consider making this requirement explicit in the contract**). Where the processor is required by law to disclose information, they still need to inform you but are not seeking your permission. The only exception to this is where the law also requires that your organisation (as controller) is not informed about the disclosure. Such a case might arise where access to information held by the processor is required by a court order, where the data controller is the subject of an investigation.

Contract clauses should be added for compliance to the NDG Data Security Standards where a standard NHS contract (which is already populated with appropriate clauses) is not being used.

What responsibilities and liabilities do processors have in their own right?

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR, a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.
- If a processor fails to meet any of these obligations or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Due diligence

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.

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 (https://ccsagreements.cabinetoffice.gov.uk/contracts/rm3764ii)

NHS Digital contracts for/supplies a number of IT systems and solutions in use by multiple NHS organisations. Please note that NHS Digital ensures in each of its system procurements that appropriate data security certifications are in place from its suppliers.

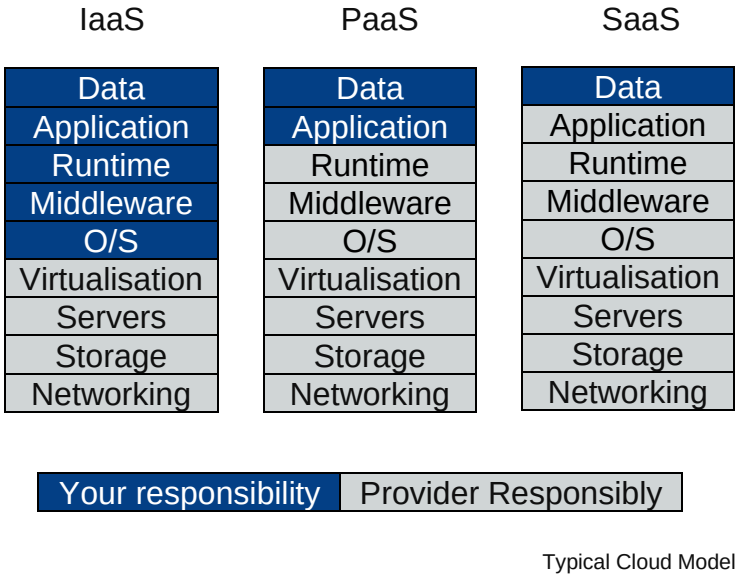
Source: https://improvement.nhs.uk/documents/2643/17-18_DSPR_Statement_of_Requirements_-_QUESTIONS_11April.pdf

Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

Data Security Standard 10.2.1

Outsourced responsibility

Services such as the cloud is a good example of where there is a shared responsibility of support between the customer and provider.



Typical Cloud Model

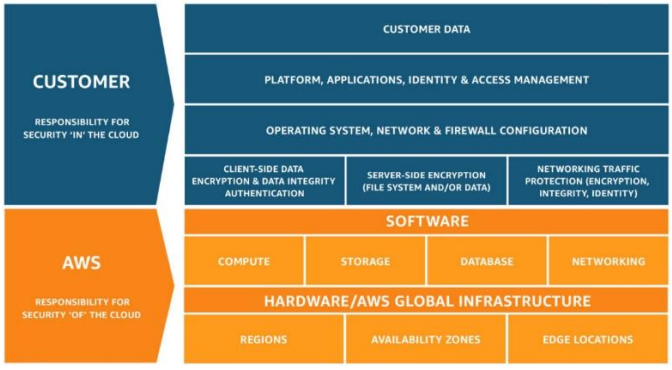
The three cloud models above IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) have varying levels of responsibility between yourself and your provider.

This is very different from the past with an on-premise servers which could be a challenge to support but very clear on your responsibilities. It is important to know where your responsibilities end and your providers' begin to ensure nothing falls beneath the gaps and responsibilities are clearly outlined and documented in your contracts.

The different models are discussed here

https://www.ncsc.gov.uk/collection/cloud-security/separation-and-cloud-security

In execution there will differences in how cloud suppliers deliver their models for example see Amazons AWS shared responsibility model below.



AWS Shared Responsibility Model
https://aws.amazon.com/compliance/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.

> Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.
>
> Data Security Standard 10.2.4

Suppliers / data processors / joint controllers completing a toolkit

Where any suppliers, data processors or joint controllers processes (processing includes viewing) personal confidential information, ensure that they have completed a data security and protection toolkit.

If not, they should be able to demonstrate an equal or higher standard.

Suppliers completing the DSPT can self-assert that they reached the data security standard. This allows a level playing field to a known standard.

> All Suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.
>
> Data Security Standard 10.2.5

Managing supplier incidents

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 that meet the threshold as being reportable / notifiable, as well as ones that are beneath that bar.

The vast majority of incidents from processors will be reported without undue delay to the controller. However remember that under 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

List of data security incidents – past or present – with current suppliers who handle personal information.

Data Security Standard 10.3.1

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

Where you as an organisation are 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 any GDPR readiness;
- 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).

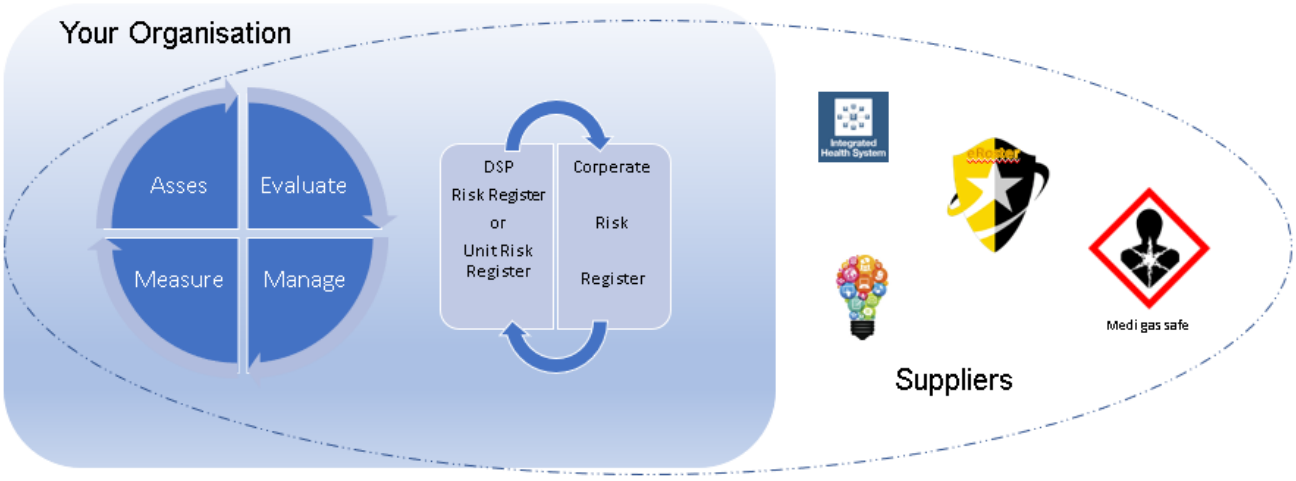
List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.

Data Security Standard 10.4.1

Risk

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

Suppliers can have an effect on the delivery of your services which in turn can affect individuals' rights and freedoms. Therefore, you have to extend your risk management process to those suppliers involved in the networks and information systems. This can either be viewed from as a supply chain issue or a GDPR processing view. The results are the same i.e.to have risk assurance.



Supplier View

GDPR View

With a little help from your friends

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

Where appropriate, you offer support to suppliers to resolve incidents.

Data Security Standard 10.5.1

Appendix 1 -
Table of Data Security Level 10 Assertions

Assertion	Sub Assertion	Evidence
10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations.	10.1.1	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.
	10.1.2	Contracts with all third parties that handle personal information are compliant with ICO guidance.
10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance.	10.2.1	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.
	10.2.3	Percentage of suppliers with data security contract clauses in place.
	10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.
	10.2.5	All Suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.
10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.	10.3.1	List of data security incidents – past or present – with current suppliers who handle personal information.

10.4 All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at board	10.4.1	List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.
10.5 The organisation understands and manages security risks to networks and information systems from your supply chain.	10.5.1	Your organisation's approach to risk management includes the risks to your services arising from supply chain.
	10.5.2	Where appropriate, you offer support to suppliers to resolve incidents.

Appendix 2 - Useful resources

Cyber security risks in the supply chain: National Cyber Security Centre

An introduction to cyber security risks in supply chains and also provides examples to highlight the benefits of an inclusive approach.

https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain

Guide to GDPR accountability and governance contracts: Information Commissioner's Office

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

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).

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

GDPR guidance contracts and liabilities between controllers and processors: Information Commissioner's Office

These pages sit alongside our overview of the GDPR and provide more detailed, practical guidance for UK organisations on contracts between controllers and processors under the GDPR.

https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

GDPR checklist: Information Commissioner's Office

Use our checklists to assess your compliance with data protection law and find out what you need to do to make sure you are keeping people's personal data secure. Once you have completed each self assessment checklist a short report will be created suggesting practical actions you can take and providing links to additional guidance you could read that will help you improve your data protection compliance.

https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/

Appendix 3 –
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