Data Security Standard 1

Personal confidential data

The bigger picture
and how the standard fits in

2019/20

Information and technology
for better health and care

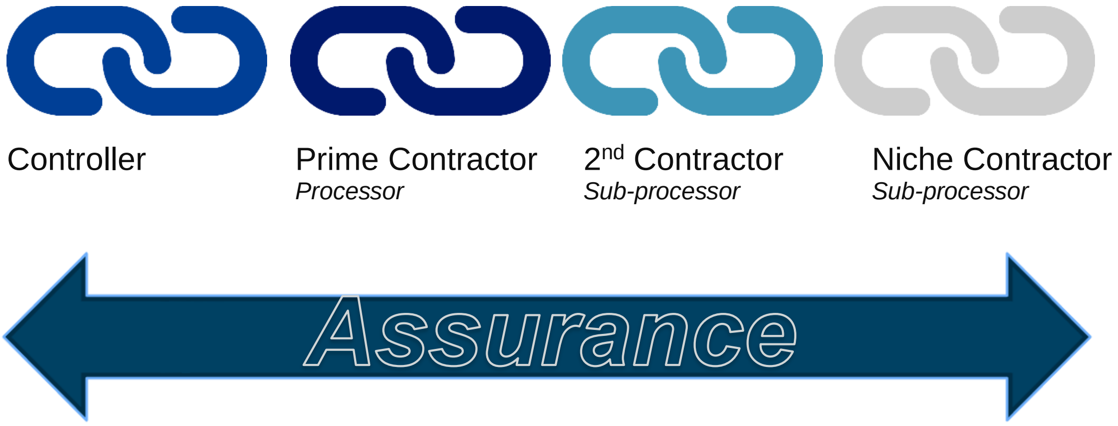
Contents

Overview

The NDG's review data standard 1 Personal confidential data, states that

"All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form."

Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained in the relevant pieces of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal confidential data.



Controller

Prime Contractor
Processor

2nd Contractor
Sub-processor

Niche Contractor
Sub-processor

> NB This guidance is not designed to be an authoritative single source of truth on all things GDPR related but does explain the assertion requirements and the question they pose.

Leadership

Tone from the top of your organisation

The National Data Guardian review showed how having the right people engaged in senior data security and protection roles can make a significant difference.

The individual roles at a senior level that are relevant are those of the SIRO and Caldicott Guardian.

Neither role is new. Both remain as valid today as when they were first conceived.

However, since the creation of the SIRO role following the Cabinet Office review and report on data handling in 2008, the landscape has changed significantly.

In 2008, the information risks were mostly centred on sensitive information held on unencrypted media and sent by fax, and with paper patient records and the manual processes they involved.

Cyber activity was lower, and health and care not seen as a worthwhile target.

“The Review heard that a strong Senior Information Risk Owner (SIRO) makes a significant difference, and that Caldicott Guardians have had a positive impact where they have been properly supported. These established positions are viewed positively and can help to ‘ensure organisational buy-in. However, there was some concern that other Board members would assume that security was something dealt with exclusively by the Caldicott Guardian or SIRO and therefore responsibility was not spread more widely, particularly in large organisations. The board as a whole should take responsibility.”

NDG Review

Senior Information Risk Officer role

The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the board (or equivalent senior management group/committee). The SIRO may also be the Chief Information Officer (CIO) if the latter is on the board, but should not be the Caldicott Guardian, as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a board member already leading on risk management or information governance.

The SIRO will act as an advocate for information risk on the board and in internal discussions and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

The SIRO is responsible for authorising access to national systems https://digital.nhs.uk/services/organisation-data-service/our-services#SIRO

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management strategy and processes. He/she will provide leadership and guidance to a number of Information Asset Owners.

The key responsibilities of the SIRO are to:

- oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework.
- take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
- review and agree action in respect of identified information risks.
- ensure that the organisation’s approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff.
- provide a focal point for the resolution and / or discussion of information risk issues.
- ensure the board is adequately briefed on information risk issues.
- ensure that all care systems’ information assets have an assigned Information Asset Owner.

Has SIRO Responsibility for data security been assigned?

Data Security Standard 1.1.1

Caldicott Guardian role

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

All NHS organisations and local authorities providing social services must have a Caldicott Guardian who is required to be registered on the publicly available National Register of Caldicott Guardians. Other health and social organisations (e.g. from the independent sector) are encouraged to register a Caldicott Guardian.

To update your organisation’s details on the Register, please visit the NHS Digital website to complete the registration form at: https://digital.nhs.uk/services/organisation-data-service/our-services#CG

Please note the form MUST be submitted from the mailbox of an Authorised Signatory. Authorised Signatories for different organisation-types are set out on the form.

Data Protection Officer

The EU General Data Protection Regulation (GDPR) came into effect in UK Law from 25 May 2018. While the GDPR will not be directly applicable post-Brexit, the Government has confirmed that it will still apply. GDPR is supplemented by the Data Protection Act 2018 and they must be read alongside each other to understand much of the law regarding data protection in the UK.

Do we need to have a Data Protection Officer?

Under the GDPR, you **must** appoint a Data Protection Officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- your core activities include large scale regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities include large scale processing of special categories of data (which includes information relating to an individual’s health) or data relating to criminal convictions and offences.

So, organisations such as General Practices, dental practices and pharmacies, and particularly those that carry out NHS work, will probably need to appoint a DPO.

There has been an accepted amendment of organisations that are not classified as public authorities (where a DPO is not required), however this amendment is limited to parish councils in England.

No health and care organisations have been exempted from the DPO requirement.

What should I do now?

Assume you will need a DPO or have access to the services of one, e.g. through pooling of resources or shared services.

The role and characteristics of a DPO

The GDPR does not clarify exactly what qualifications a DPO should have. They should have experience working in and expert knowledge of data protection law. Ideally, they will also know the sector well.

The DPO's responsibilities include:

1) Informing and advising organisations about complying with GDPR and other data protection laws;

2) Monitoring compliance with GDPR and data protection laws – including staff training and internal audits;

3) Advising on and monitoring data protection impact assessments;

4) When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.

5) Cooperating with the Information Commissioner's Office (ICO);

6) Being the first contact published point for the ICO and citizens in terms of data processing.

It will be difficult for smaller providers to appoint a DPO internally because of the position the DPO must occupy in the organisation. The GDPR specifies that the DPO must not receive instructions on how to carry out their tasks relating to data processing, that they cannot be dismissed or penalised for performing their tasks and that they must report directly to the highest level of management.

Additionally, the DPO cannot be the individual who decides the means and purposes of processing data in your organisation. For example, a manager plans to bring in a new rota system which would include staff personal details; they couldn't also be the DPO because the decision-making process might conflict with data protection obligations.

There is more information about requirements for DPOs here:

Information Governance Alliance: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance and

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

Can we assign other tasks to the DPO (such as IG Manager)?

The GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Information / Cyber Security/ Lead / Manager

This role can vary from a very technical one managing data controls to more a general security assurance developing and maintaining an Information Security Management System.

It can be a full-time role but is sometimes shared with other roles such as the Information Governance (IG) Lead, or an IT Manager.

The role and characteristics of Information / Cyber Security/ Lead / Manager

There is no universally agreed responsibilities but typically these would include:

1) Informing and advising and implementing an organisation’s security posture including the effectiveness of security controls.

2) Monitoring compliance / certification with a range of legislation and standards which could include Network and Information Systems (NIS) Regulations, the security elements of GDPR data protection laws, Cyber Essentials, ISO 27001 and the Data Security and Protection Toolkit (DSPT) itself.

3) Responding and coordinating the response to CareCert alerts and advisories.

4) Responding to and coordinating efforts to security related incidents

5) Cooperating with NHS Digital, the ICO and National Cyber Security Centre (NCSC);

6) Being a champion and advocate for good information security practise in the organisation.

The link below provides some useful resources for managing a cyber security;

See https://digital.nhs.uk/services/data-security-centre

What about IG Leads?

Information Governance Leads in larger organisations will probably merge with the more formal role of Data Protection Officer. There is still an expectation that the following duties will be carried (irrespective of the name of the role):

Information Governance Leads in larger organisations may merge with the more formal role of Data Protection Officer (DPO), however where this is the case there must be no conflict of interest with the DPO's primary tasks

1. A representative from the senior level of management should be appointed to act as the overall Information Governance Lead and co-ordinate the IG work programme.

2. The Department of Health and Social Care's response to the Caldicott 2 and 3 Reviews contains an expectation that organisations across health and social care strengthen their leadership on information governance through ensuring that Caldicott Guardians or IG Leads, Senior Information Risk Owners and appropriate information governance staff are in place, trained and have time to focus on information governance.

3. Under the approved arrangements, the IG Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks of an IG Lead include:

a. developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high-level strategy document supported by corporate and / or directorate policies and procedures;

b. ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;

c. providing direction in formulating, establishing and promoting IG policies;

d. establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;

e. ensuring annual assessments using the DSPT and audits of DSPT policies and arrangements are carried out, documented and reported in line with the requirements of the NHS Standard Contract;

f. ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the board or senior management team, in a timely manner. For example, for NHS Trusts, sign off may be scheduled in advance of the end of financial year submission on the 31 March each year;

g. ensuring that the approach to information handling is communicated to all staff and made available to the public;

h. ensuring that information governance staff understand the need to support the safe sharing of personal confidential data for direct care as well as the need to protect individuals' confidentiality;

i. All three documents can be downloaded from the Big Picture Guides in the help section Knowledge Base Resources;

j. liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;

k. monitoring information handling activities to ensure compliance with law and guidance;

l. providing a focal point for the resolution and/or discussion of IG issues.

m. ensuring that appropriate training is made available to all staff and completed as necessary to support their duties.

For NHS organisations, this will need to be in line with the mandate for all staff to be trained annually and should take into account the findings of the National Data Guardian's Review of Data Security, Consent and Opt-outs' and ensure people can make informed choices about how their data is used. 'Information: To Share Or Not To Share? The Information Governance Review

https://www.gov.uk/government/publications/the-information-governance-review

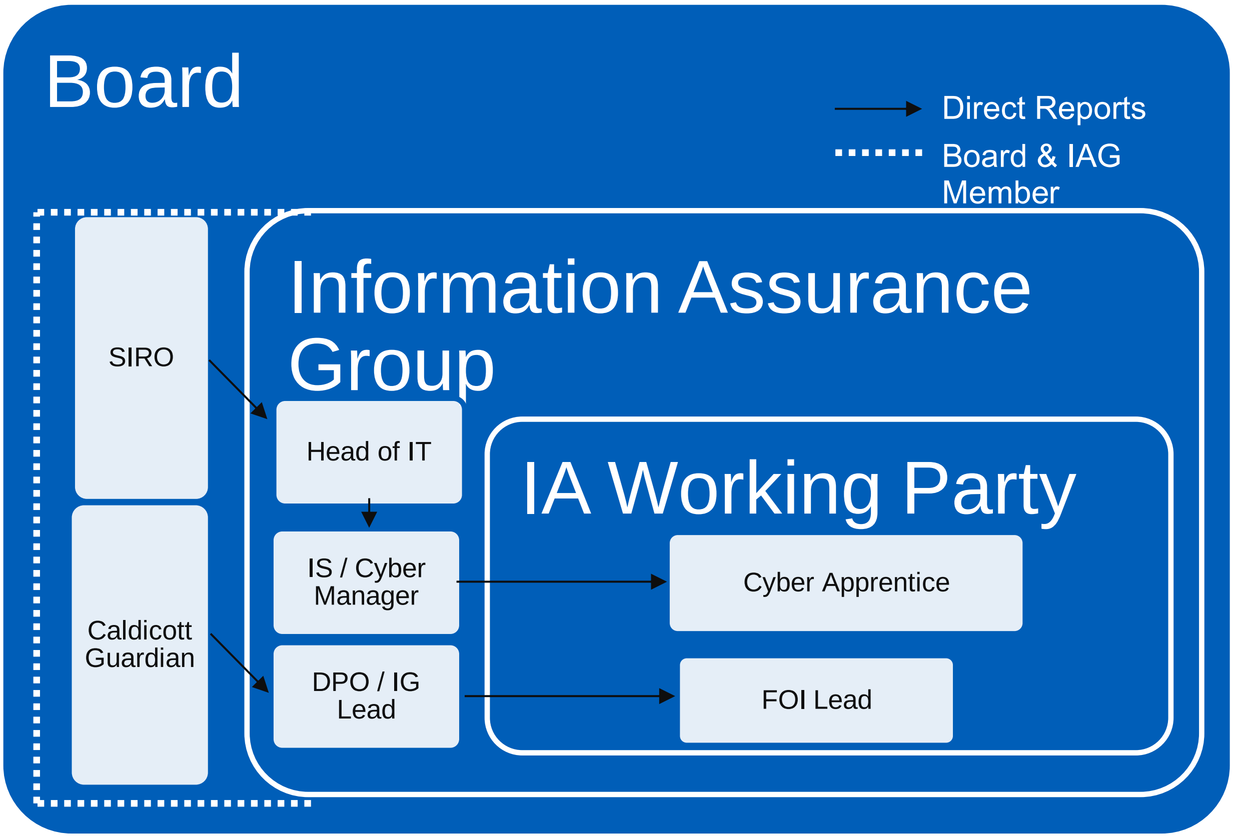
The Information Governance Review, informally known as the 'Caldicott2 Review'; and the Government's response to the Review.

More information on the roles and responsibilities is available in the Key Roles and DPO Guide

Lines of accountability and responsibility and direction

There should a be a clear line of accountability and responsibility between the roles involved in the delivery of your organisation's data security approach. It should be transparent, well defined and documented showing the lines of accountability and responsibility from the specialist roles to the board.

An example of this type of clarity is below.



The direction set by the board should be disseminated throughout the organisation through its policies, projects and procedures.

For example, using the structure above, a board's concern for data security is exfiltration from staff members' social media postings which may lead to a board level Social Media policy sponsored by the SIRO and ratified at the Information Assurance group. This then leads to purchasing a more granular web filtering / data loss product. The responsibility for management is delegated to the Information Security / Cyber Manager and reflected in their job description. Part of this management is reflected in a weekly process to examine a social media exceptions report which is carried out by the cyber apprentice.

Are there clear lines of responsibility and accountability to named individuals for data security?

Data Security Standard 1.1.3

Is data security direction set at board level and translated into effective organisational practices?

Data Security Standard 1.1.4

Policies

Policies for data security and protection are one of the foundations to having a framework in place for data security and protection.

The different sizes and complexity of organisations means that some will have one all-encompassing policy, whilst others may have multiple policies supported by standards and procedures.

There is no set number of how many different policies you have on these topics, but it is important the policies are effective, acknowledged and understood. However, they should be Board approved i.e. sponsored at Board level and ratified at a steering group with delegated authority.

It is also important they:

- are reviewed at regular intervals
- are your "live" policies and finalised (i.e. not draft)
- are version controlled
- have not gone past their review date
- follow your approved process for policy ratification (like all your other policies) including SIRO endorsement
- where appropriate, are linked to other corporate policies (such as an acceptable use policy linking to a disciplinary policy)
- are available to staff and the public.

In terms of the topics, it is recommended that your policy(s) should cover at least the following:

- data protection including confidentiality
- Freedom of Information (if the organisation is subject to the Act)
- data security
- records management
- acceptable use.

The relevant guidance in focus will depend on the topic e.g. Data Protection IGA/ICO guidance, Cyber / Data Security NHS Digital and National Centre for Cyber Security

Are there Board approved data security and protection policies in place that follow relevant guidance?

Data Security Standard 1.2.1

Individuals’ rights and the Regulator

Regulator - the Information Commissioner

Under the previous DPA 1998, data controllers were required to pay a registration fee and provide the ICO with details about the types of processing they were carrying out.

The GDPR, supplemented by the Data Protection Act 2018, removes the requirement to notify the ICO of the types of processing. A fee will still be payable as the Government has introduced the Data Protection (Charges and Information) Regulations 2018 to coincide with GDPR, which contain a new three-tier funding model. The ICO has provided guidance on the new funding model, which will assist organisations to determine which tier of the funding model they fall into: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/guide-to-the-data-protection-fee/

Controllers that are required to pay a fee, will also be required to provide the following details to the ICO:

- the name and address of the controller (for registered companies, this should be the address of its registered office; for any other person carrying on a business, this should be that person’s principal place of business in the UK)
- the number of members of staff
- the turnover for your financial year
- any other trading names the organisation has
- the name and contact details of the person completing the registration process
- a relevant person in the organisation (or another relevant representative) whom the ICO can contact on regulatory matters (for example, renewing the data protection fee when it is due), if this is a different person from the above
- if the organisation is required to have a DPO, details of who that person is (if this is different from the above).

Individuals’ rights

GDPR embeds the principle of transparency and promotes the objective of strengthening individuals' rights, accountability, and the lawful and fair processing of data.

Individuals’ rights must be respected and therefore your internal processes should support individuals to exercise those rights.

Please see IGA GDPR checklist (9. Support individuals’ rights).

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

Transparency

GDPR contains stringent transparency requirements in Articles 13 and 14 to support people being properly informed of the use of their personal information and of their rights, before or at the time their information is collected.

Please see IGA GDPR checklist (7. Comply with more stringent transparency requirements).

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance .

How are Data Security and Protection Policies available to the public?

Data Security Standard 1.2.3

Informing Individuals

Transparent processing is fundamental to individuals being able to exercise rights when their personal data is being processed. Individuals can be informed directly via correspondence or indirectly through the use of leaflets and websites, which must be brought to their attention.

Your transparency information should include the personal data collected, the purpose, the lawful basis for processing, a list of rights and when/whether they apply to the processing undertaken by the organisation, contact details and procedure for subject access requests, and other rights requests.

For a full list of what your transparency information should include please see the ICO guidance:

How is transparency information (e.g. your Privacy Notice) published and available to the public?

Data Security Standard 1.3.2

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

and the IGA GDPR checklist (7. Comply with more stringent transparency requirements).

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

How have Individuals been informed about their rights and how to exercise them?

Data Security Standard 1.3.3

Subject access

Under GDPR/DPA 18, there is no charge for Subject Access Requests, unless the request is manifestly unfounded or excessive, or an individual requests further copies of their data following a request where you may charge a “reasonable fee” for the administrative costs of complying with the request.

You must act on the subject access request without undue delay and at the latest within one month of receipt.

For more information on Subject Access Requests see the ICO guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

and /or the IGA GDPR checklist (10. Manage subject access requests).

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

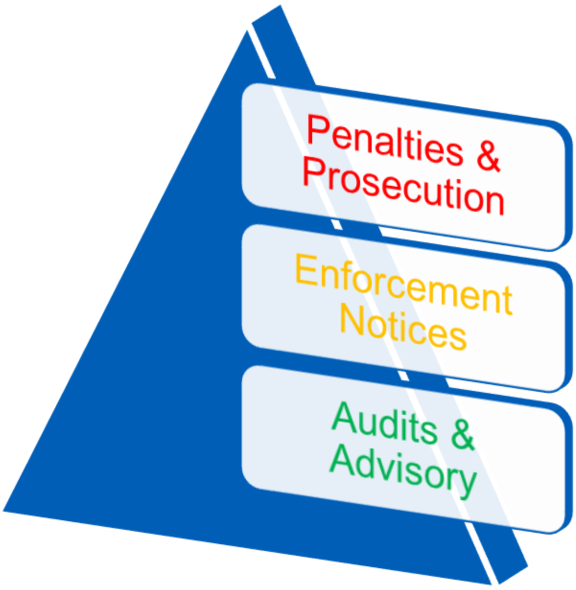
You will need to provide evidence of the number of Subject Access Requests you have received and that they have been responded to in the relevant timescales. Especially note if any requests were answered late. If Freedom of Information Requests apply to your organisation, then provide these details too. You can put context around any lateness (e.g. staff absence etc) but predominantly all that is required is the figures.

For period dd/mm/yy to dd/mm/yy	
No of SARs	nn
No of SARs late	nn
No of FOI	nn
No of FOI late	nn

Organisations' interaction with the ICO

GDPR/DPA 18 Interactions

The ICO has three levels of interactions with organisations covering data protection:



Penalties and prosecution

The most serious action the ICO can take involves monetary penalties or prosecution.

https://ico.org.uk/action-weve-taken/enforcement/

Enforcement notices

Deemed less serious than monetary penalties, an enforcement notice would lay out a course of action the organisation should do to correct a deficiency(s) in data protection law. The enforcement notice actions are normally signed off by the chief executive of the organisation that requires improvement. Enforcement notices can lead to monetary penalties if the required actions specified in the enforcement are not undertaken.

https://ico.org.uk/action-weve-taken/enforcement/

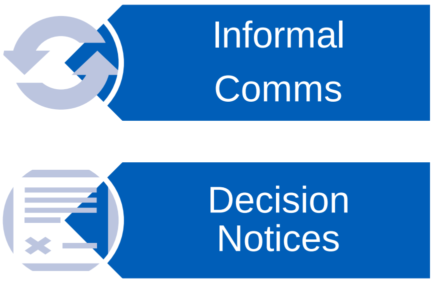
Audits and advisory

Audits and advisory can be self-initiated and are seen as demonstrating how an organisation can improve its data protection compliance. They are not binding, like enforcement notices. ICO action does not include audits and advisory visits and there is no requirement to mention those.

https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/

Freedom of Information

The ICO has one primary interaction with organisations covering freedom of information:



Informal Comms

Decision Notices

Decision Notices

In the relation to freedom of information requests where a complaint is not resolved informally the ICO will issue a decision notice, if they find the organisation has breached the Freedom of Information Act.

ICO action (for the purposes of the DSPT) does not include informal communication but does cover decision notices on information and environmental information cases.

Have there been any ICO actions taken against the organisation in the last 12 months, such as fines, enforcement notices or decision notices?

Data Security Standard 1.3.5

Data flow mapping (Article 30 register of processing activities)

There must be a record (e.g. register or registers) that details each use or sharing of personal data, including the legal basis for the processing and if applicable, whether the National Data Opt-Out has been applied to any sharing of confidential patient information for secondary purposes.

The record should include for each entry:

Purpose of processing, legal basis relied on from GDPR Article 6 and Article 9, categories of data subject / personal data, categories of recipients, whether personal data is transferred overseas, whether personal data is retained and disposed of in line with policies, or if not, why not, and whether the National Data Opt-Out is relevant to the sharing. Whether a written data-sharing agreement or contract is in place and when it ends.

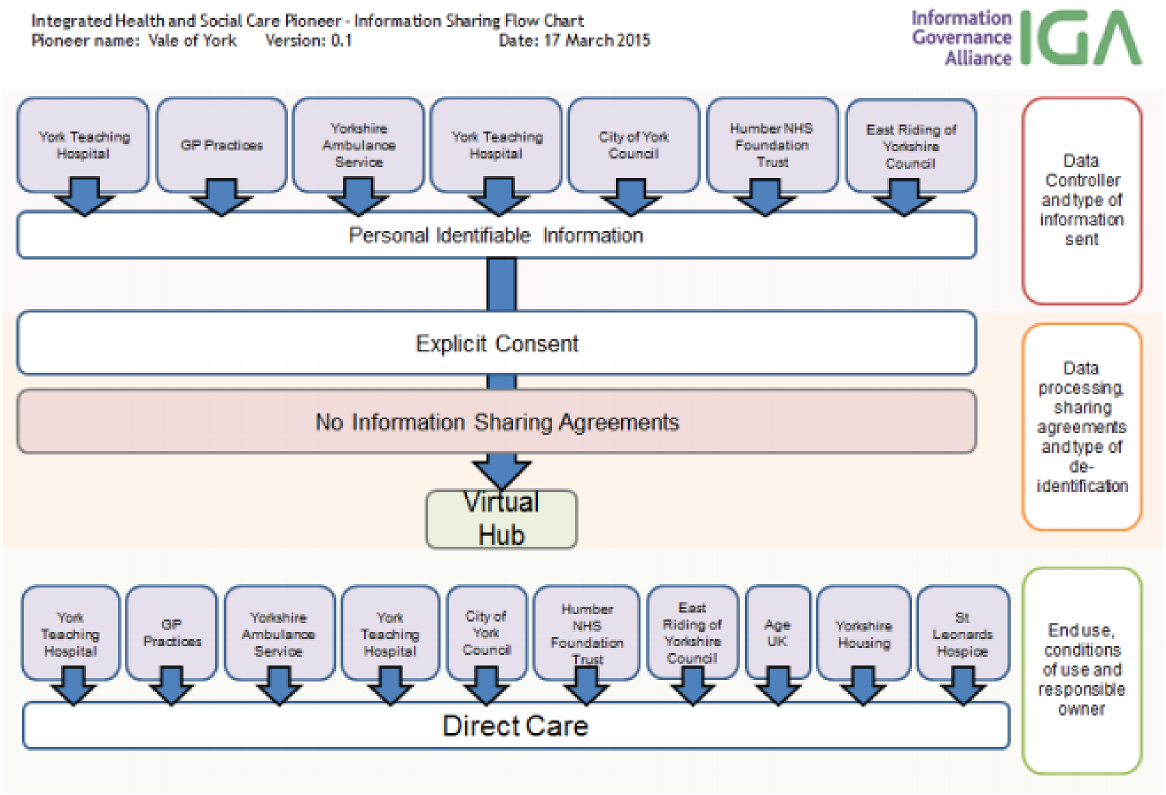
Provide details of the record or register that details each use or sharing or personal information.

Data Security Standard 1.4.1

Understanding what data will flow between organisations is one of the fundamental building blocks of good information governance. Until data flows have been captured and mapped, they cannot be effectively risk assessed and secured against known risks.

One of the key considerations associated with data flow mapping is to understand the legal basis for each flow.

As well as a register, it may be helpful to generate a high-level map of the sharing between organisations, not at the individual data flow level, but just to map that there are such flows. This provides at a glance clarity which may also support engagement with senior staff, partner organisations and service user communications, such as one from the IGA.


Integrated Health and Social Care Pioneer - Information Sharing Flow Chart
Pioneer name: Vale of York Version: 0.1 Date: 17 March 2015
Information Governance Alliance IGA
York Teaching Hospital
GP Practices
Yorkshire Ambulance Service
York Teaching Hospital
City of York Council
Humber NHS Foundation Trust
East Riding of Yorkshire Council
Personal Identifiable Information
Data Controller and type of information sent
Explicit Consent
No Information Sharing Agreements
Virtual Hub
Data processing, sharing agreements and type of de-identification
York Teaching Hospital
GP Practices
Yorkshire Ambulance Service
York Teaching Hospital
City of York Council
Humber NHS Foundation Trust
East Riding of Yorkshire Council
Age UK
Yorkshire Housing
St Leonards Hospice
Direct Care
End use, conditions of use and responsible owner

The flows themselves need SIRO and board approval or equivalent senior management roles in the organisation.

There are some examples of asset / data flow templates in the Secondary Use Data Governance Tool (SUDGT) website

https://data.england.nhs.uk/sudgt/

When were information flows approved by the Board or equivalent?

Data Security Standard 1.4.2

Information assets / systems

Definitions and scope

Personal confidential information (PCI) is personal and usually sensitive and confidential information that is held about staff and patients / service users.

Personal information is information about living or deceased people. In health and care settings, personal information will also be confidential as it has been given in confidence so that people can receive health and care services. It can include names and addresses as well as a person's health and care information. Confidential personal information may also be held about staff.

Confidential personal information is likely to include (but is not limited to) information about someone's:

- physical or mental health
- social or family circumstance
- financial standing and financial details
- education, training and employment experience
- religious beliefs
- racial or ethnic origin
- sexuality
- criminal convictions
- genomic data
- IP address.

Confidential personal information can be held in systems such as:

- patient administration systems
- staff rostering systems
- payroll
- theatre systems
- data warehouses
- a clinical correspondence system.

There is not a prescribed method of how this information can be recorded/held, however, this can be an existing information asset register, provided it meets the criteria of including details of:

The type, location, software, owner, support and maintenance arrangements, quantity of data and how critical they are to the organisation and if applicable, whether the system / information asset falls under the NIS Directive.

Provide a list of all systems/information assets holding or sharing personal information.

Data Security Standard 1.4.3

National Data Opt-Out

Following on from recommendations of the National Data Guardian Report: Review of Data Security, Consent and Opt-Outs, and the subsequent Government Response: Your Data: Better Security, Better Choice, Better Care, a new national data opt-out has been developed. It provides a simple, accessible way for the public to opt out of their confidential patient information being used for purposes other than their individual care and treatment. Key messages on the roll out of the national data opt-out are:

- The public were able to set national data opt-outs from 25th May 2018.
- NHS Digital and Public Health England are already compliant and are applying national data opt-outs.
- Other health and social care organisations will be required to implement by 2020.
- The planned timeline for providing support to help organisations become compliant is as follows:
    - National organisations – October 2018-March 2019
    - NHS trusts – February-August 2019
    - GP practices and clinical commissioning groups – May-October 2019
    - Local authorities and adult social care – April 2019-March 2020
    - others such as pharmacies, NHS dental and NHS optician services – October 2019–March 2020

- Health and social care providers need to be prepared to handle enquiries from patients/service users regarding the national data opt-out.-. Information and resources are available to organisations on the NHS Digital website.

  https://digital.nhs.uk/national-data-opt-out

Is your organisation compliant with the national data opt-out policy?

Data Security Standard 1.4.4

Data protection guidance and monitoring

There is approved staff guidance on confidentiality and data protection issues. In line with the organisation’s data protection policy, there is guidance for staff on using and sharing personal information in accordance with data protection legislation, common law duties, and professional codes and national data opt-outs, e.g. staff code of conduct, national data opt-out model guidance and Data Protection Impact Assessment (DPIA) guidance etc.

This can range from general awareness campaigns:

https://ico.org.uk/for-organisations/resources-and-support/posters-stickers-and-e-learning/

to detailed guidance and procedures, such as variants as those produced by the IGA website

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources

Is there approved staff guidance on confidentiality and data protection issues?

Data Security Standard 1.5.1

Spot Checks

You should also undertake spot checks and audits to see whether the staff guidance on confidentiality and data protection is being adhered to.

The organisation should ensure that it has assigned overall responsibility for monitoring and auditing access to confidential personal information to an appropriate senior staff member, e.g. the Caldicott Guardian, IG Lead or equivalent. This member of staff should be responsible for ensuring that confidentiality audit procedures are developed and communicated to all staff with the potential to access confidential personal information. The procedures should include:

- how access to confidential information will be monitored;
- who will carry out the monitoring of access;
- reporting processes and escalation processes;
- disciplinary processes.

The following are examples of events that the organisation should audit for frequency, circumstances, location etc:

- failed attempts to access confidential information;
- repeated attempts to access confidential information;
- successful access of confidential information by unauthorised persons;
- evidence of shared login sessions/passwords;
- disciplinary actions taken.

Every organisation that has access to Summary Care Records (SCRs) must have a nominated Privacy Officer Function that is responsible for monitoring the SCR viewing activity of their users to check whether SCR views were legitimate. Individuals with the Privacy Officer role will be given access rights on their Smartcard to perform the activities necessary to manage alerts and audit SCR viewing activity.

Alerts are generated by end users when they override one of the information governance controls that are in place. Therefore, activities that will trigger an alert include:

- When a clinician self-claims a legitimate relationship - Create Legitimate Relationship (Self Claimed) Alert.
- Emergency access of SCR (i.e. without gaining permission, e.g. patient unconscious or confused) –
- Dissent Override Alerts (for integrated systems) and SCR Dissent Override Alerts (for SCR Application or SCRa).

What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?

Data Security Standard 1.5.2

Data protection and security by design and default

Systems should be designed to take account of data protection and security issues at the point of conception. Trying to retrofit controls to systems that have little consideration at the onset can be expensive, labour intensive and less seamless to the users of the systems.

Your data protection by design and default procedures should aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent where feasible allowing individuals to monitor what is being done with their data and restricting settings to ensure systems aren’t accessible by default to an indefinite number of persons.

Together the procedures should enable your organisation to improve data protection and security.

You should have a procedure that sets out the organisation’s approach to data protection by design and by default, which includes pseudonymisation requirements. This should cover your existing systems and accessing new systems.

It should cover the full lifecycle of systems from genesis to retirement and disposal. All the storage, access and transmission (data at rest and in motion) should also be addressed.

Please see IGA GDPR checklist (3. Data protection by design and default and DPIAs).

> There is an approved procedure that sets out the organisation’s approach to data protection by design and by default, which includes pseudonymisation requirements.
>
> Data Security Standard 1.6.1

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

This procedure should be approved through your local governance process.

Technical and physical access controls

It important that only the people who are intended to see, access, modify and delete data do so and not others.

There are generally two methods: technical and physical access controls.

Technical controls can include (but are not limited to):

- Role based access

  Having accessed based on your role to only access the information you need for the role.

- Least privileged

  Have the minimum amount of rights to access systems to carry out your role.

- Smartcard enabled access

  Using smartcard and other forms (token etc.) of physical to introduce another factor in accessing systems.

- Encryption

  Both of data at rest (where it is stored) and in motion.

- Endpoint port control

  Control access to USB (and other ports) particularly on end points to control who and what data is copied to and from them.

- Pseudonymisation techniques

  Where appropriate only using data sets that are anonymised or pseudonymised for systems (particularly for non-care).

  https://ico.org.uk/media/1061/anonymisation-code.pdf

- Using test data (where appropriate)

  Using data that is completely unrelated to live data, such as for training.

- Data loss prevention

A system that inspects data going outside the organisation and can report and / or block it.

- Control of personal web-based email systems

One method to circumvent organisational controls is to use commercial web-based email systems to upload corporate data. Controlling access to web-based mail can be an effective control.

- Effective audit logging

Although a reactive control (post event), it can be used as a deterrent and help inform development of new technical controls.

There are technical controls that prevent information from being inappropriately copied or downloaded.

Data Security Standard 1.6.2

Physical controls.

Those physical measures that restrict access to areas and data sources only to people that are authorised.

These can include (but is not limited to).

- lockable doors, windows and cupboards
- clear desk procedures
- identification ID
- key card access
- code locks for secure areas.

There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.

Data Security Standard 1.6.3

Data protection by design audit

An audit should be undertaken within the reporting year to review the implementation of technical controls i.e. pseudonymisation and anonymisation or de-identification, access controls, encryption, computer port controls as well as physical controls.

The audit should include findings and provide details of any remedial actions that should occur. The information recorded on the DSPT should be at the headline finding level with anything that could impact your data security and protection redacted.

Provide the overall findings of the last data protection by design audit.

Data Security Standard 1.6.4

Data protection impact assessments

DPIAs are used by organisations to identify, understand and address any risks to privacy that might arise when developing new products and services or undertaking any other new activities that involve the processing of personal data.

Under GDPR, organisations should undertake DPIAs where their planned processing involves high risk processing:

'High risk processing' encompasses:

- automated processing
- large scale processing of special categories data - which includes health and genetic data
- systematic monitoring of a public area, such as through the use of CCTV

Examples include :-

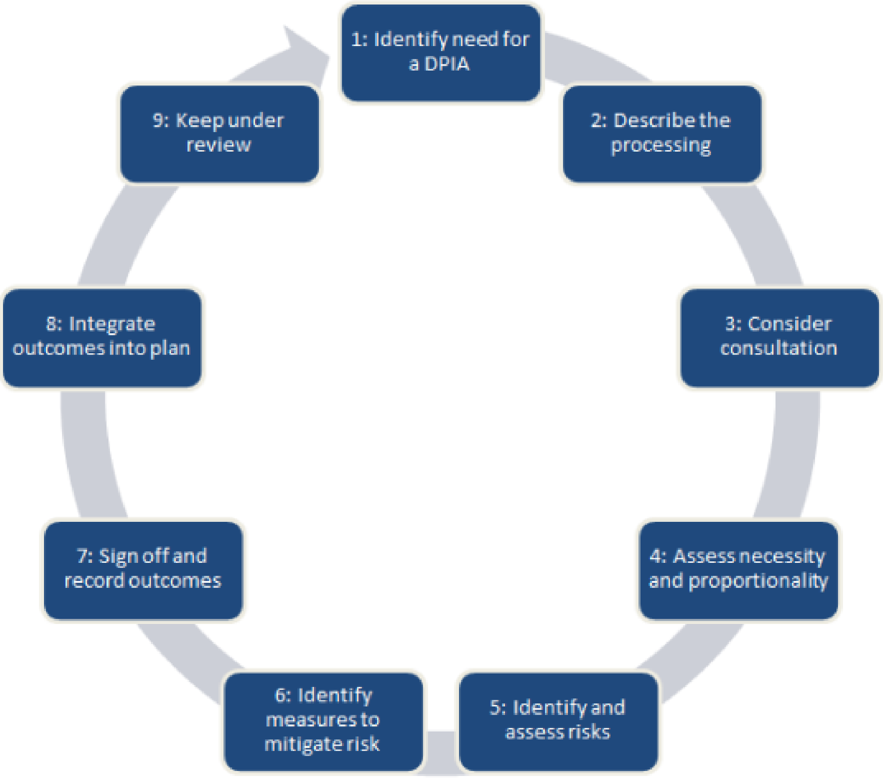
- Innovative technology
- Denial of Service (not a cyber attack)
- Large scale profiling
- Biometric data
- Genetic data
- Data matching
- Invisible processing
- Tracking
- Marketing / Profiling children or vulnerable indivduals
- Risk of physical harm

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

The GDPR also requires DPIAs to be undertaken if planned data processing activities are otherwise "likely to result in a high risk to the rights and freedoms of natural persons"

If there is an existing process, it should be reviewed having regard to the circumstances in which a DPIA should be undertaken and noting the GDPR requires:

- seeking the advice of the DPO when carrying out an assessment
- consulting with the ICO where a DPIA indicates a high risk to individual rights and freedoms that cannot be mitigated.


1: Identify need for a DPIA
2: Describe the processing
3: Consider consultation
4: Assess necessity and proportionality
5: Identify and assess risks
6: Identify measures to mitigate risk
7: Sign off and record outcomes
8: Integrate outcomes into plan
9: Keep under review

The process should be compatible with ICO guidelines (such as the process above). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

Please see IGA GDPR checklist (3. Data protection by design and default and DPIAs) https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The process should be agreed at board or equivalent level.

It is important that the DPIA process is challenging, probing and systemic and should have the goal of identifying new risks that may not have an associated mitigation.

It also important that the DPIA forms part of your data protection by design and any possible high-risk processing assessment occurs before processing commences

If your DPIA identifies a high risk and you cannot mitigate that risk, you must consult the ICO **before** starting the processing. The ICO has stated that written advice will be provided within eight weeks, or 14 weeks in complex cases.

Is a Data Protection Impact Assessment carried out before high risk processing commences?

Data Security Standard 1.6.6

The ICO has a regulatory sandbox the first phase is detailed here

https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/

In some circumstances ,where the ICO has significant concerns, the ICO may impose a limitation or ban your intended processing.,.https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/

As part of the data protection transparency agenda, DPIAs should be published, though they should be redacted of any sensitive information that may have a security risk.

Have any unmitigated risks been identified through the Data Protection Impact Assessment process and notified to the ICO?

Data Security Standard 1.6.7

Data Protection Impact Assessments are published and available as part of the organisation’s transparency materials.

Data Security Standard 1.6.8

Data quality

For the purpose of the toolkit data quality is split into two items.

- Data Quality Assurance
- Clinical Coding

Data Quality Assurance –data quality issues can be introduced at any stage in the lifecycle of the data and so it is important to be able to assure the data throughout its journey. This starts with the publication of an information standard and associated Technical Output Specification that describes what good data looks like and ends with data quality reports issued by NHS Digital at the point of submission and publication. In the Data Quality Assurance section below, we explore the key internal and external resources that can be used to assure the quality of data at source.

Clinical Coding - is a health administration function that involves the translation of written clinical statements into a nationally and internationally recognised coded format. A clinical coder will analyse information about an episode of patient care and assign standardised alphanumeric codes for both diagnoses and procedures/interventions using the relevant classification system.

Coded clinical data is audited against national clinical coding standards. A clinical coding audit must be objective and provide value to the local organisation by highlighting and promoting the benefits of taking remedial actions to improve data quality and processes as well as acknowledging evidence of best practice.

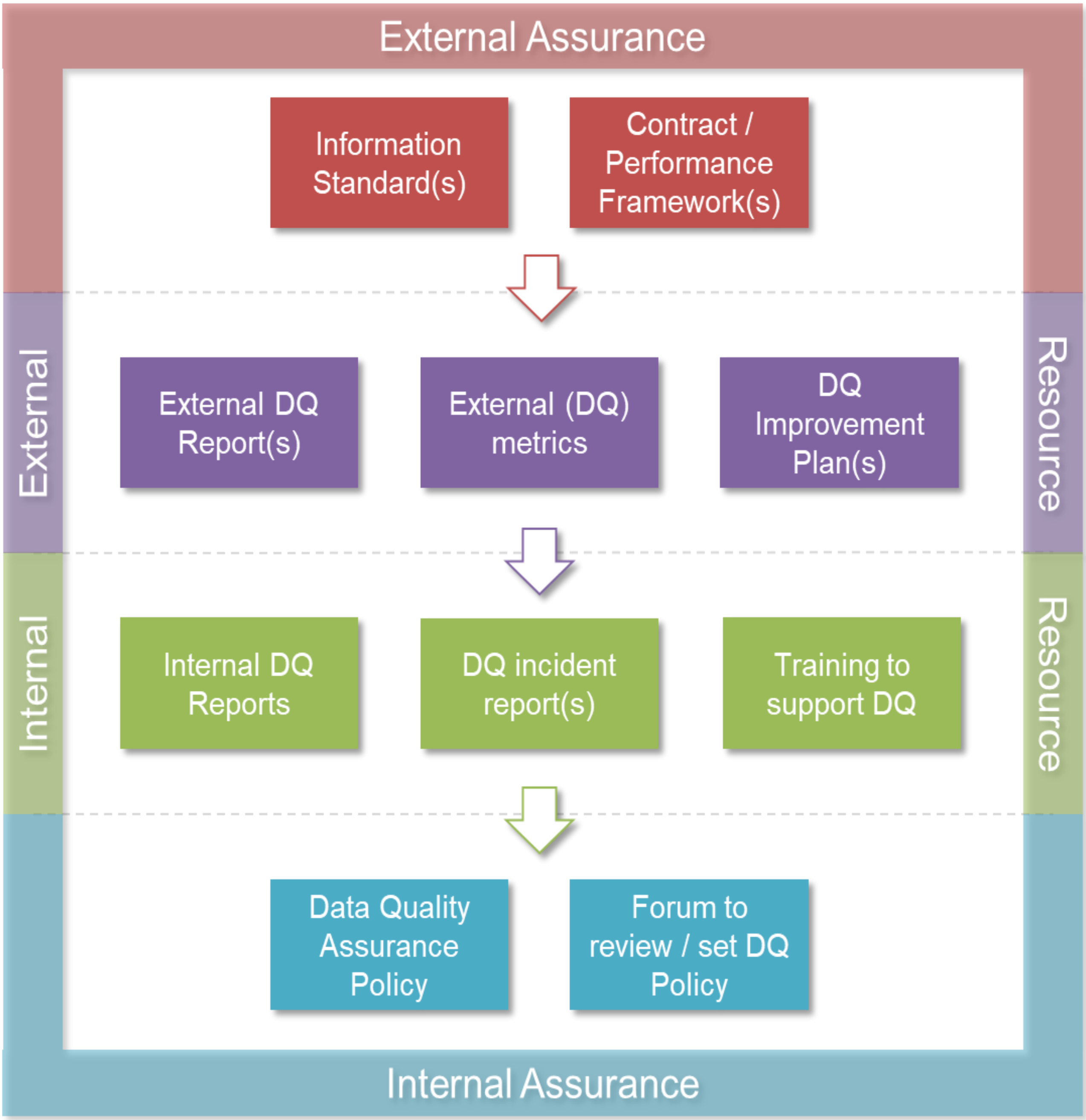
When there are documentation discrepancies or recurring reporting issues which are outside the remit or control of the clinical coding department, the audit report should highlight these to be addressed through the local information governance and clinical governance arrangements.

Local coding policy and procedure documents should be inspected as part of a clinical coding audit to ensure these:

- are up to date
- evidence local agreements and implementation
- have been applied consistently
- do not contravene national clinical coding standards.

Data Quality

This guidance is intended to cover the wider topic of data quality assurance. The diagram below depicts a range of external data quality sources and related resources that should be used to inform what related internal policies and resources are required to support this assertion.



Each topic in the diagram is explored in more detail in the remainder of this document.

Where additional formal guidance or documentation is available links will be included within the guidance.

This is not a complete list of data quality resources / products available for assurance purposes, however, it should be considered the minimum required to support this assertion.

External Assurance / Resources

Information Standards

Each provider should ensure all systems are compliant with all relevant information standards published by NHS Digital on the Information Standards website and that their systems suppliers have implemented all applicable standards and are similarly compliant.

National definitions and guidance support the sharing, exchange and comparison of information across the NHS and other care providers. Common definitions, known as information standards, are used for commissioning purposes, to support comparative data analysis, for the preparation of performance tables, for data returns to the Department of Health and Social Care and also support clinical messages, such as those used for pathology and radiology.

National information standards should not just be seen as supporting the collection of data on a consistent basis throughout the NHS and other care providers. They also have an important role in supporting the flow and quality of information used, so that health and care professionals are presented with the relevant information where and when it is required to provide effective care and treatment to service users.

Organisations should ensure that:

- Electronic systems have built in data quality checks which are conformant with, or map to national Data Standards (where these exist);
- For the relevant service user information systems, where national data standard definitions and values exist:
    - values on the key systems match the national standard definitions;
    - no other values are used unless these are mapped explicitly for central returns;
    - the number and combination of alpha/numeric digits within a code match the format of the NHS Data Dictionary and the code conforms or maps to a nationally determined coding structure (where these exist).

Organisations should also have policies / procedures to ensure:

- Validation routines are used routinely on data entry to assure completeness and validity of datasets, both those used locally and for central returns;
- Standard definitions used in data schemas on key systems, checking all entries on the schema relating to these definitions against national definitions and codes;
- Monitoring in place to identify and resolve duplicate records.

Performance Framework(s)

There are a number of key contractual and performance frameworks in place that have a data quality component within them designed to monitor and improve data quality at source. These include:

- **NHS Standard Contract** –Schedule 4, Service Condition 28 and Schedule 6 of the NHS Standard Contract each contain data quality elements. Schedule 4 contains metrics relating to completeness of the NHS Number and Ethnicity coding in national datasets such as the Secondary Uses Services (SUS) dataset and the Mental Health Services Dataset (MHSDS). Part B of Schedule 6 and Service Condition 28 defines how commissioners should use Data Quality Improvement Plans (DQIPs) to monitor critical data quality issues.

- **Single Oversight Framework** – NHS Improvement's Single Oversight Framework currently contains a Judgement Metric based on NHS Digital's Data Quality Maturity Index (DQMI) for providers of Mental Health Services. This will be extended across other providers types in 2019/20.
- **Model Hospital** – NHS Improvement use the DQMI as a metric within the Model Hospital.
- **CQC Well-led Domain** – The CQC collect data quality metrics through their Insight portal as part of the Provider Information Request (PIR) stage of an inspection. This includes the DQMI.

Each of the above frameworks should be reviewed to determine both national and local contractual and performance obligations relating to data quality including:

- Monitoring of the DQMI is in place to ensure scores are held at recommended thresholds and issues identified and resolved.
- Establishing DQIPs where data quality issues are identified and monitoring these through appropriate contract review mechanisms to ensure improvements achieved.
- Any contractual obligations relating to data quality are 'passed through' to sub-contractors and vendors alike.

External Data Quality Reports & Metrics

There are a number of externally published data quality reports and metrics that should be used to support local data quality assurance and improvement activities. These include:

- The Data Quality Maturity Index (DQMI) published by NHS Digital and based on 8 key national datasets including the main three Commissioning Datasets (CDS), Mental Health Services Dataset (MHSDS) and the Maternity Services Dataset (MSDS).
- The SUS DQ Dashboards published monthly by NHS Digital for the three Commissioning Datasets (CDS); Admitted Patient Care (APC), Outpatients (OP) and Emergency Care (ECDS) - registration is required.
- The Hospital Episode Statistics (HES) Data Quality Notes published regularly by NHS Digital contains additional data quality information following additional processing on the three Commissioning Datasets (CDS) submitted through the Secondary Uses Service (SUS).
- National dataset specific data quality reports published at point of submission by NHS Digital through the Bureau Services Portal for collections such as Mental Health Services Dataset (MHSDS), Maternity Services Dataset (MSDS) and the Community Services Dataset (CSDS).
- Dataset specific data quality reports (on both local and national datasets) processed by Data Services for Commissioners (DSfC) and issued via Commissioning Support Units (CSUs) and supplied direct or via commissioners
- Third party services from organisations who use open data published by NHS Digital and other health care bodies to provide benchmarking and clinical coding assurance tools

Organisations should use all available external resources to assure and improve the quality of their data by:

- Downloading all available data quality reports to identify point of submission errors and correct prior to submission deadlines;

- Gaining access to applicable data quality dashboards to identify and correct additional data quality issues within a timely manner;
- Investigating other external data quality sources and adopting where applicable

The above should be reflected in local data quality policies and procedures (see Internal Assurance) to ensure that data quality reports on the organisation's data from external sources are followed up and appropriate corrections made, with an effective feedback loop to staff to help prevent similar mistakes being made in the future.

The Board / senior management or delegated sub-committee / group should be kept aware of progress. Action plans for improvement should be signed off by the delegated sub-committee/group or senior management, and appropriate resources will need to be applied to ensure the success of these.

Data Quality Improvement Plans

A Data Quality Improvement Plan (DQIP) is a component of the NHS Standard Contract available to commissioners to detail known or emerging data quality issues within a provider’s national or local data flows and specify a set of corrective actions. The commissioner can then use the established contract review process to monitor progress against the DQIP. Schedule 6 Part b of the NHS Standard Contract (Particulars) sets out the structure of a DQIP including what data quality issue is being measured, what the threshold of achievement is, how it will be measured, by when the threshold should be achieved and the consequences of not meeting it. It is to be recommended to commissioners that from 2019/20 the Data Quality Maturity Index (DQMI) is included as standard in all DQIPs to provide focus on data quality and allow the use of existing contract review processes to monitor compliance.

Other External Resources

Data Dictionary

Organisations must ensure that all data held in local systems and subsequently submitted to national systems conforms to the NHS Data Dictionary (where applicable).

The number and combination of alpha/numeric digits within a code must match the format specified in the NHS Data Dictionary and codes must conform or map to a nationally determined coding structure.

Data Validation

Organisations should ensure that all local systems have built in data quality checks which are conformant with, or map to, national Information Standards where these exist.

Point of entry validation should be applied to local systems and should be built into system supplier developments where possible.

All systems used to deliver healthcare, including third party supplier systems, locally developed systems or local configurations of third-party systems must be compliant with all relevant information standards and must conform to the NHS Data Dictionary.

For relevant service user information systems, where national data standard definitions and values exist, values used in these systems data schemas must match the national definitions and values. No other values should be used unless these are mapped explicitly for central returns.

Tracing

Organisations should make use of all available tracing services, such as the Personal Demographic Service (PDS) and the Demographic Batch Service (DBS) to ensure a suitable level of accuracy is attained for person level data. Data items used for PDS tracing should be regularly assessed for quality to ensure the correct details are being traced.

Internal Resources

Internal DQ Reports

Organisations should ensure that all data submitted through local and national data portals, such as the Secondary Uses Service (SUS+), Bureau Services Portal and Data Landing Portal accurately reflects the care a patient received.

Documented procedures should be in place for reporting on and analysing the quality of information in local systems prior to and after submission of central returns and reports. This should include:

- Reconciliation activities between data held in local clinical systems and reporting systems to ensure data extraction processes do not introduce data quality issues prior to submission.
- Regular monitoring of national and local data quality reports, with evidence of specific highlighted data quality issues being corrected or Data Quality Improvement Plans (see External Assurance) being put in place to resolve more complex issues.
- Regular monitoring of national data quality metrics such as the Data Quality Maturity Index (DQMI), SUS DQ Dashboards and associated KPI reports, with evidence of receipt and action taken to address key issues or Data Quality Improvement Plans (see External Assurance) being put in place to resolve more complex issues.

Where data quality monitoring is undertaken by a third party on behalf of the organisation, such as a shared health informatics service, then the precise roles and responsibilities of all parties should be clearly documented within a service level agreement (SLA). Third party assurance statements should be sought from the auditors of the service provider on the controls in place for data quality at the service.

DQ Incident Reports

Organisations should have procedures for handling incidents relating to their data, including data quality issues, and these should be defined within the organisations Data Quality Policy (see Internal Assurance).

Incident systems should be used to capture all relevant details relating to reported incidents allowing for audit, learning and review to be completed on reported incidents.

All data quality related incidents should be investigated by the Data Quality Team (or equivalent) and reviewed by the Data Quality Steering Group (or equivalent) to ensure that lessons learned are used to inform updates to the Data Quality Policy, systems configuration and / or staff training.

The Caldicott Guardian for an organisation should regularly review all data quality incidents and provide additional guidance on specific incidents where appropriate.

Training

All staff should receive appropriate data quality training and awareness sessions to ensure that they understand the importance of collecting and recording complete and accurate information to minimise the risks to the service user and to the organisation itself. The use of examples and scenarios may be particularly useful to ensure that a basic level of competence has been achieved before access to the systems is allowed.

Some staff within organisations may be required to have higher levels of awareness relating to data quality to carry out their duties. Where this is the case appropriate additional training should be provided according to staff job roles, level of access to person identifiable information and responsibilities for processing/managing records.

The training programme must cover all aspects of data quality including:

- The definition of individual data items - so that staff know what they are recording;
- The eventual use of data – so staff understand what the data they are recording will eventually be used for (and therefore why it is important to record accurately);
- The function of data items – so staff know the purpose of recording;
- How to validate data with the service user or against the health care record – so checks are carried out to confirm the accuracy of data.

The need for data quality training should be reflected in the organisation's Data Quality Policy (see Internal Assurance) and compliance monitored through the Data Quality Steering Group (or equivalent) who should also regularly review the training material to ensure it is up-to-date.

Internal Assurance

Data Quality Policy

Each organisation should have a Data Quality Policy be that a standalone document or part of a wider IT governance policy. The policy may also be referenced from other related polices such as that for Information Governance or Health Records Management. The policy should detail data quality related responsibilities for all staff directly involved in the collection and input of clinical and non-clinical data.

The Data Quality Policy should as a minimum include the following:

- **Purpose and scope of the policy**: its intended use and what and who it covers
- **Key principles**: defines the underlying drivers for data quality, links to organisational objectives / values and links to other key organisational strategies and policies
- **Roles and responsibilities**: defines the key roles covered by the policy from the board downwards and their respective responsibilities in delivery against the policy
- **Data Quality Standards and Audit:**: defines what data quality is in the context of the organisation and how it will be assured
- **Data Standards**: makes reference to internal and external assurance resources such as the NHS Data Dictionary and Data Security & Protection Toolkit
- **Measurement of Good Data Quality**: defines what dimensions will be used to measure data quality e.g. completeness, validity and integrity
- **Validation and Quality Assurance**: details all the internal and external resources that will be used to assure data quality e.g. DQMI, SUS DQ Dashboards, submission DQ reports and benchmarking tools
- **Training and Support**: details what training is available / mandated for data quality
- **Supporting Documentation**: lists internal Standard Operating Procedures and other policies that directly impact data quality
- **Monitoring Data Quality**: defines how data quality is monitored and through which groups / boards it will be reported
- **Communication**: details which channels will be used to communicate on data quality issues
- **Policy Dissemination and Implementation**: defines how the policy will be shared
- **Monitoring Policy Compliance and Effectiveness**: defines through what processes and activities the organisation will monitor compliance with the policy.

Data Quality Group

To support the Data Quality Policy (or in some instances to create the policy in the first instance) there should be a formal group established to review and monitor compliance with the policy. This may take the form of a Data Quality Steering Group or a sub-group within the established IT governance structure such as an Information Governance Group. The group should have in place a formal Terms of Reference that sets out the following:

- **Purpose**: the strategic objectives of the group as informed by the Data Quality Policy.
- **Duties and responsibilities**: what it will monitor, discuss and take decisions on in the context of data quality.
- **Accountability**: who in the organisational governance structure it is accountable to e.g. Information Governance Group.
- **Links to other groups**: what other groups or boards it has dependencies on or have dependencies on it within the organisation e.g. Health Records Management Group
- **Membership**: list of members including the Chair and Secretary and what constitutes a quorate meeting.
- **Inputs and Outputs**: what the main inputs and outputs are of the meeting and their respective contributors and recipients.
- **Frequency of meetings**: how often the group will meet and any dependencies / constraints

Data Quality Team

Depending on the size of the organisation there may be the need / opportunity to create a dedicated Data Quality Team either within the Information Services Department or within a Quality / Performance structure.

The scope and responsibilities of the team should include:

- **Policy**: Contributing to the development and implementation of data quality related policies.
- **Process**: Defining data quality processes in line with the Data Quality Policy.
- **Reporting**: Collating and actioning DQ Reports issued by NHS Digital (national flows) or DSCRO / CSU (local flows) as appropriate.
- **Metrics**: Monitoring of KPIs and other performance related metrics such as the DQMI for underlying DQ issues.
- **Improvement**: Delivering against Data Quality Improvement Plans (DQIPs) as defined by CCGs or NHS England (Specialist Commissioning) and as identified through internal sources.
- **Governance**: Attending the Data Quality Steering Group (or equivalent) as required.
- **Incidents**: investigating root cause of DQ incident investigation (from Incident System) and feeding learning into training and / or systems validation as appropriate.
- **Training**: Defining data quality related training requirements (from central sources or through incident management) and delivering regular training to staff.
- **Expertise**: Providing subject matter expertise on all national and local data flows.

Clinical Coding

Overview

There are established procedures in place at Acute and Mental Health Trusts for regular quality inspections of the coded clinical data for inpatient and day case episodes by Approved Clinical Coding Auditors using and applying the latest version of the Terminology and Classifications Delivery Service' Clinical Coding Audit Methodology to demonstrate compliance with the clinical classifications OPCS-4[1] and ICD-10[2], associated national clinical coding standards[3], and the organisation's commitment to continual improvement of its coded clinical data. **NB:** For Mental Health Trusts, this Standard only covers data recorded for submission to the Admitted Patient Care (APC) Data Set and the requirement for OPCS-4 collection is only where the organisation's Patient Administration System has the functionality to collect OPCS-4 codes.

These clinical coding audits must be undertaken by a Terminology and Classifications Delivery Service Approved Clinical Coding Auditor. The results including findings, conclusions and recommendations of all clinical coding audits conducted within the last 12 months are noted by the organisation and there must be documented evidence that any recommendations have been actioned/progressed by the organisation.

Guidance

Robust Data Quality and Clinical Coding Audit Programme

Introduction

1. Organisations[4] and clinical coding staff depend on clear, accurate coded clinical data in order to provide a true picture of patient hospital activity and the care given by clinicians. Coded clinical data is important for a number of reasons, for example:
    - monitoring provision of health services across the UK
    - research and monitoring of health trends
    - NHS financial planning and payment
    - clinical governance.
2. The Terminology and Classifications Delivery Service provides a working NHS-wide model for carrying out coded clinical data audits, including those undertaken at Independent Sector Treatment Centres.

Audit Programme – Data Quality (Clinical Coding)

3. Data Quality Audit, focused on clinical coding, is a crucial part of a robust assurance framework required to support the provision of accurate and statistically meaningful

[1] OPCS-4 Classification of Interventions and Procedures Version 4.8 (2017) – the procedure/intervention classification in use in the UK by members of the clinical coding profession.
[2] ICD-10 – International statistical classification of diseases and related health problems (10th revision)
[3] National Clinical Coding Standards ICD-10 5th Edition and OPCS-4 reference books Terminology and Classifications Delivery Service
[4] Organisation in this context is referring to both NHS and non-NHS organisations responsible for the delivery of patient care.

coded data to facilitate the information and clinical governance agendas for both payment and the development of electronic care records.

a. A programme of clinical coding audits focused on data quality in accordance with the guidance set out below.

   This programme may be in the form of, either:

   i. a continuous clinical coding audit programme comprising several small audits undertaken throughout the course of the year as part of routine maintenance of standards (see also 14b);

   ii. a single one-off audit, which should be undertaken every twelve months.

The number of finished consultant episodes (FCEs) audited must be a minimum of 200 FCEs for Acute Trusts and 50 FCEs for Mental Health Trusts. (See also 14b)

Data Quality (Clinical Coding) Audit Specification

4. For the purposes of this requirement, clinical coding audits are performed as part of a continuous data quality programme. The audits must be based on the current version of the service Clinical Coding Audit Methodology and be undertaken by a service approved clinical coding auditor who has complied with all of the requirements of the Terminology and Classifications Delivery Service Clinical Coding Auditor Programme. The auditor may or may not be employed by the organisation but must abide by Caldicott Guardian requirements. The overall % accuracy scores should be greater than or equal to the levels indicated in the guidance below.

5. Documented evidence that recommendations made in previous clinical coding audits have been noted and actioned must be made available to the auditor.

6. Organisations should routinely undertake audits of their data as part of good practice in keeping under review their performance in providing good quality data (refer to the detailed guidance provided in the Approved Clinical Coding Auditor Code of Conduct).

The Terminology and Classifications Delivery Service Clinical Coding Audit Methodology

7. In order to monitor the quality of coded clinical data, organisations should adopt a procedure for regular audit, review and improvement. This should incorporate processes to ensure recommendations made at audit are tracked through to completion and must be made available to the auditor.

8. The aim of the audit is to check that clinical coding processes are in place and to ensure the inputted data complies with national clinical coding standards. Coded clinical data will always be audited against the national clinical coding standards. Any clinical data that cannot be referenced against ICD-10 Volumes 1-3, OPCS-4 Volumes I-II, the National Clinical Coding Standards ICD-10 5th Edition reference book, the National Clinical Coding Standards OPCS-4.8 reference book, the National Tariff Chemotherapy Regimen List, the National Tariff High Cost Drugs List, Chemotherapy Regimens Clinical Coding Standards and Guidance, High Cost Drugs Clinical Coding Standards and Guidance or the Coding Clinic will not be pursued.

9. Generally mental health clinical coding is undertaken by professional clinical coders who are fully knowledgeable in the national clinical coding standards of both ICD-10 and OPCS-4. However, the Terminology and Classifications Delivery Service

recognises that some Mental Health Trusts do not employ dedicated clinical coders who have been provided with training in all aspects of these classifications and that the recording of coded clinical data may be captured using other methods. Therefore, provisions have been put in place, and this Data and Security Protection Toolkit Standard takes into account that Mental Health Trusts may now be using electronic records (e.g. EPR) and that audits will be performed based on the data available in the full clinical record, whether this is a paper or an electronic version.

10. The Clinical Coding Audit Methodology describes the full range of analyses that are carried out on all diagnosis and procedure codes. These include analysis of both primary and secondary diagnosis and procedure codes for:

- correct and incorrect codes
- incorrect sequencing of codes
- irrelevant codes and omitted codes.

11. A summary of the Methodology titled ‘A Guide to Clinical Coding Audit Best Practice’ is available for reference by non-Approved Clinical Coding Auditors.

12. The clinical coding audit also examines the process undertaken for coding and the documentation (either paper or electronic) available for use during the coding process.

13. Selection of the sample for the audits may be informed by the results of national benchmarking and/or previous audits. Other examples include clinical specialty specific audits or a general sample which is representative of the case-mix, specialty and type of admission of the organisation. The clinical coding auditors have a responsibility to satisfy themselves that the sample is random within this constraint.

14. For clinical coding audit, the requirements for achieving attainment of mandatory and advisory for clinical coding analysis within information quality assurance are that:

    a) Organisations should have carried out a clinical coding audit programme within the last twelve months* prior to submission of the Information Quality Assurance scores for this version of the Data Security and Protection Toolkit.

    b) The approved auditor must have met and complied with all requirements of the Clinical Coding Auditor Programme (CCAP) and adhered to the latest version of the Terminology and Classifications Delivery Service’ Clinical Coding Audit Methodology and the Approved Clinical Coding Auditor Code of Conduct.

    The minimum requirement for an **Acute Trust** is for coding audits totalling **a minimum of 200*** Consultant Episodes (or 2%*, whichever is the smaller) to be undertaken over the year either as a one-off audit, or as a series of smaller audits that add up to a minimum of 200 Consultant Episodes (or 2% if smaller) to assure the quality of information as part of a local audit programme.

    The minimum requirement to assure the quality of information as part of a local audit programme for a **Mental Health Trust** is for coding audits totalling **a minimum of 50** Consultant Episodes.

    *Beyond this published minimum, each organisation needs to decide a meaningful number of consultant episodes to be audited across each of its sites and specialities in order to underpin its data quality. This should be discussed by members of the organisation’s Data Quality team.

c) Within the report there should be an analysis of reasons for the errors identified, which distinguish between coder and non-coder error. For example, whether the error is due to the incorrect code assigned or due to problems with documentation or process not being fit for purpose. However, for the purposes of information quality assurance, an error due to either cause would be regarded as an inaccuracy. Organisations are urged to note that many issues with clinical coding may arise not from the coders, but from problems with the information given to the coders to code from, and that these will need to be addressed.

d) Organisations should use the analysis contained in their clinical coding audit reports to understand the reasons behind any errors and ensure that any recommendations made in the previous clinical coding audits have been noted and actioned. The auditor will ask to see those documents which evidence that recommendations from previous audits have been tracked to completion, for example, an Action Log or Audit Tracker, changes within the Clinical Coding Departmental Policy and Procedure document etc.

e) The Terminology and Classifications Delivery Service provides the following percentage accuracy scores:

Acute Trust

	Level of Attainment	
	Standards Met	**Standards Exceeded**
Primary Diagnosis	>=90%	>=95%
Secondary Diagnosis	>=80%	>=90%
Primary Procedure	>=90%	>=95%
Secondary Procedure	>=80%	>=90%

Mental Health Trust

	Level of Attainment	
	Standards Met	**Standards Exceeded**
Primary Diagnosis	>=85%	>=90%
Secondary Diagnosis	>=75%	>=80%
Primary Procedure*	>=85%	>=90%
Secondary Procedure*	>=75%	>=80%

***** Where systems allow the capture of OPCS-4 codes, the clinical coding must comply with national clinical coding standards.

15. Trusts must meet or exceed the required percentage across all four areas in order to meet the attainment level.

This guidance can also be found in the Data Security Standard 1 Data Quality: Clinical Coding Audit Guidance – Acute and Mental Health Trusts on Delen.

There is a policy and staff guidance on data quality.

Data Security Standard 1.7.1

Data quality metrics and reports are used to assess and improve data quality.

Data Security Standard 1.7.2

A data quality forum monitors the effectiveness of data quality assurance processes.

Data Security Standard 1.7.3

Records Management

As part of your records management policy and CQC standards, you should have record management guidance that supports your records management policy which covers the full spectrum of the function of records and media you deal with (including but not limited to):

Function:

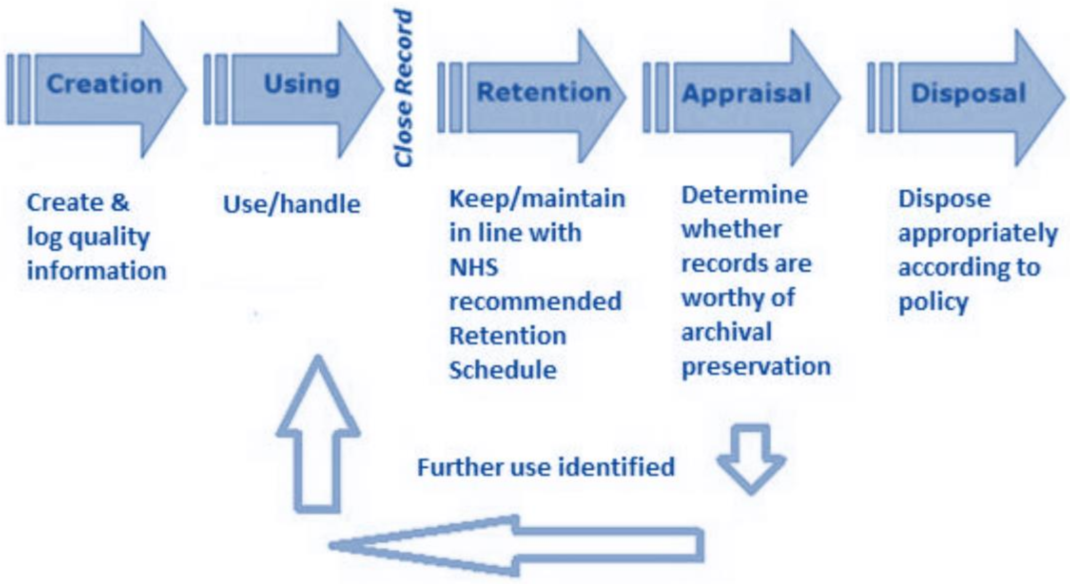
- patient health records (electronic or paper based, including those concerning all specialties and GP records)
- records of private patients seen on NHS premises
- accident & emergency, birth, and all other registers
- theatre registers and minor operations (and other related) registers
- administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling)
- X-ray and imaging reports, output and images
- integrated health and social care records
- data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.
- a patient or staff genomic data or IP address.

Format:

- photographs, slides, and other images
- microform (i.e. microfiche/microfilm)
- audio and video tapes, cassettes, CD-ROM etc
- emails
- computerised records
- scanned records
- text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter® and Skype®
- websites and intranet sites that provide key information to patients and staff.
- Manual Records (such as case notes)
- Electronic Records (such as patient administration system)
- pictures and videos (Dicom images, ultrasound recordings).

The records / information lifecycle

Your records management framework should manage the records lifecycle, or the information lifecycle, which is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest (for those subject to the Public Records Act or FoI).


Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log quality information
Use/handle
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of archival preservation
Dispose appropriately according to policy
Further use identified

Arguably the biggest concern (from a data security and protection viewpoint) is towards the end of the lifecycle. There are plenty of high profile cases where records have been inappropriately disposed of, leading to a data breach or alternatively disposed of earlier than they should have been.

Consequently, it is important to have a guidance for staff setting out the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived. This should be supported by a records retention schedule.

Both these documents should take account of the "*Records Management Code of Practice for Health and Social Care 2016*".

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Has a records retention schedule been produced?

Data Security Standard 1.7.4

Data disposal

Your data disposal contracts and suppliers should reference or include guidance on disposal of electronic media containing personal or sensitive data

https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/sanitisation-reuse-disposal-and-destruction-of-electronic-media-guidance-for-health-and-care-organisations

Traditionally, paper-based disposal has consisted of simple vertical shredding. However, this method is not suitable for sensitive or confidential information.

The HMG Information Assurance Standard (IS5) requires the shredding of paper records be conducted using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm. This standard is in line with the requirements of BS EN 15713:2009 and is therefore recommended for the destruction of sensitive information.

Incineration processes may also be used to dispose of paper records and other types of printed media. A certificate of destruction from a specialist waste disposal contractor is required on completion.

The contracts themselves should be reviewed periodically as the devices (and their nature) that are disposed of will change over the course of the contract. e.g. A photocopier with multiform printer that retains images of printed documents..

If third parties are used to dispose of (destroy or archive) personal data, there should be a contract in place that includes the requirement to have appropriate security measures in compliance with data protection law and the facility to allow audit by the organisation.

There should be an audit that should occur periodically on data disposal contracts. The type of items that should be included in that audit are:

- onsite inspection of the contractor disposal site ensuring sufficient physical segregation of different customer disposal items
- observing the disposal journey from asset receipt to disposal and certification
- tracing a recently collected disposed of item(s) to track where they are in the disposal journey and how they are secured (especially if mid journey).
- if the items are to be recycled, examining a finalised refurbished asset for any data remnants
- ensuring paper records are secured and adequately reference
- verifying the employment checks on a dip sample of employees from the disposal company
- tracing a dip sample of assets’ chain of custody documentation from collection to destruction and certification
- observing physical destruction of media.

Each disposed of item should be recorded on a destruction certificate.

It is important to note this data destruction can be physical (such as shredding) but can also be wiping (to the recommended standard). Each destroyed asset should be recorded on a destruction certificate. This can be one certificate per item but also can be multiple items on one certification. It is important these items are known and can be referenced individually.

So, destruction certificate with the following line item:

- 50 x SATA mixed sized hard drive destroyed - there is no traceability.Is Not acceptable

Whereas a destruction certificate with the following line item is acceptable:

- Hitachi (HGST) 500gb 500 GB 2.5 Inch 5400 RPM Sata Hard Drive (s/n 999787989ui9) status shredded.

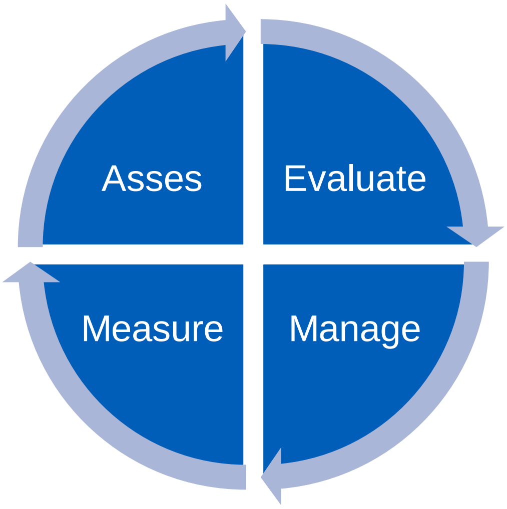
- Western Digital Scorpio Blue 500GB Sata 8MB Cache 2.5 Inch Internal Hard Drive (s/n WD21377878nh98) status shredded.

Provide details of when personal data disposal contracts were last reviewed/updated.

Data Security Standard 1.7.5

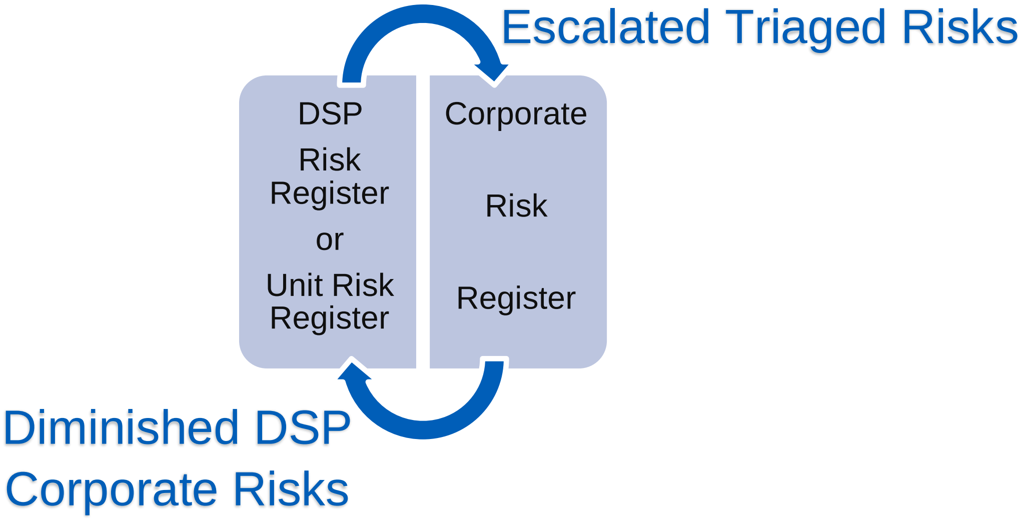
Risk Management

Management of risk is a key component of any data security and protection framework. It is important to treat risk management as a continuous cycle.



The foundation of any risk management is to capture risk and, for the data security standards , this would be those risks relating to e data security and protection.. A central dedicated data security and protection risk register may be held or form a part of multiple registers at the organisation's units/locations level.

It is also important to recognise that data security and protection risks do not exist in isolation to the rest of the organisation and they should interact with corporate risks (in a corporate risk register).



So, risks that exist on DSP risk / unit register should be escalated to the corporate risk register if they exceed your organisational threshold.

Conversely those risks that are now diminished (such as a new control is in place or the system with risk has been updated) should be relegated to its originating register (again if they now fall beneath your corporate threshold).

Please note, this guide does not endeavour to be a risk management manual - there are plenty of authoritative guides to risk, in particular the NCSC risk management collection.

https://www.ncsc.gov.uk/collection/risk-management-collection

There is not a single adopted Information Security risk management framework mandated by the DSPT. However, the framework adopted by your organisation t should be a recognised and acceptable Information Security risk management framework.

The NCSC risk management collection details some of the more common frameworks:

https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-component-driven-risk-management

Does your organisation operate and maintain a risk register that follows an acceptable Information Security risk framework which links to the corporate risk framework?

Data Security Standard 1.8.1

What are your top data security and protection risks?

As part of your risk management approach, you should holistically analyse your top risks and their underlying causes.

For example, a risk of not being able to recruit and retain data security and protection staff: The underlying cause may be issues with a lower salary range in a large urban conurbation, with a number of nearby large private enterprises paying significantly more.

Another example may be an inability to replace all legacy unsupported operating systems. This may be caused by complications with some being classified as medical devices, an IT estate not fully controlled by one group, or a lack resources either financial or staff.

Whatever your Top three risks are they should be discussed by the leaders of your organisation and plans put into place to mitigate and reduce the risk. Senior management should not just have visibility of the top three risks but any significant risks (especially those data security and protection risks on the corporate risk register).

It is important to engage with Senior Management throughout the risk management process and particularly when identifying risks and their associated mitigating actions.

What are your top three data security and protection risks?

Data Security Standard 1.8.3

Appendix 1 -

Table of Data Security Level 1 Assertions

Assertion	Sub Assertion	Evidence
1.1 There is senior ownership of data security and protection within the organisation.	1.1.1	Has SIRO Responsibility for data security been assigned?
	1.1.2	List the names and job titles of your key staff with responsibility for data protection and/or security.
	1.1.3	Are there clear lines of responsibility and accountability to named individuals for data security?
	1.1.4	Is data security direction set at board level and translated into effective organisational practices?
1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.	1.2.1	Are there Board approved data security and protection policies in place that follow relevant guidance?
	1.2.2	When were each of the data security and protection policies last updated?
	1.2.3	How are Data Security and Protection Policies available to the public?
1.3 Individuals' rights are respected and supported (GDPR Article 12-22)	1.3.1	What is your ICO Registration Number?
	1.3.2	How is transparency information (e.g. your Privacy Notice) published and available to the public?
	1.3.3	How have individuals been informed about their rights and how to exercise them?
	1.3.4	Provide details of how access to information requests have been complied with during the last twelve months.

	1.3.5	Have there been any ICO actions taken against the organisation in the last 12 months, such as fines, enforcement notices or decision notices?
1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)	1.4.1	Provide details of the record or register that details each use or sharing of personal information.
	1.4.2	When were information flows approved by the Board or equivalent?
	1.4.3	Provide a list of all systems/information assets holding or sharing personal information.
	1.4.4	Is your organisation compliant with the national data opt-out policy?
1.5 Personal information is used and shared lawfully.	1.5.1	Is there approved staff guidance on confidentiality and data protection issues?
	1.5.2	What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?
1.6 The use of personal information is subject to data protection by design and by default	1.6.1	There is an approved procedure that sets out the organisation’s approach to data protection by design and by default, which includes pseudonymisation requirements.
	1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.
	1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.

	1.6.4	Provide the overall findings of the last data protection by design audit.
	1.6.5	There is a staff procedure, agreed by the SIRO, on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.
	1.6.6	Is a Data Protection Impact Assessment carried out before high risk processing commences?
	16.7	Have any unmitigated risks been identified through the Data Protection Impact Assessment process and notified to the ICO?
	1.6.8	Data Protection Impact Assessments are published and available as part of the organisation’s transparency materials.
1.7 Effective data quality controls are in place	1.7.1	There is a policy and staff guidance on data quality.
	1.7.2	Data quality metrics and reports are used to assess and improve data quality.
	1.7.3	A data quality forum monitors the effectiveness of data quality assurance processes.
	1.7.4	Has a records retention schedule been produced?
	1.7.5	Provide details of when personal data disposal contracts were last reviewed/updated.

	1.7.6	When was the date of last audit being made on data disposal contractors/other arrangements to ensure security is of the appropriate agreed standard?
1.8 Personal information processed by the organisation is adequate (and not excessive) for the purposes.	1.8.1	Does your organisation operate and maintain a risk register that follows an acceptable Information Security risk framework which links to the corporate risk framework?
	1.8.2	Senior management have visibility of key risk decisions made throughout the organisation.
	1.8.3	What are your top three data security and protection risks?

Appendix 2 -
Useful resources

GDPR Checklist: Information Governance Alliance

A checklist for health and care organisation to assist with GDPR readiness.

https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/6/iga_-_gdpr_implementation_checklist_v1_final.pdf

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

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection. This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

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

GDPR checklist: Information Commissioner's Office

Designed to help you, as a data processor, understand and assess your high-level compliance with data protection legislation. Includes the new requirements for data processors, the rights of individuals, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Records Management Code of Practice for Health and Social Care 2016: NHS Digital

The Records Management Code of Practice for Health and Social Care 2016 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice and was published on 20 July 2016 by the Information Governance Alliance (IGA).

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Sanitisation, reuse, disposal and destruction of electronic media: guidance for health and care organisations: NHS Digital

Guidance to make sure IT equipment is cleared of sensitive data correctly before being reused and at the end of its life, so that information is appropriately protected from any unauthorised access.

Guidance covers:

- sanitisation processes
- legal requirements
- record keeping
- incident reporting and management.

https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/sanitisation-reuse-disposal-and-destruction-of-electronic-media-guidance-for-health-and-care-organisations

Risk management guidance: National Cyber Security Centre

Guidance to help organisations make decisions about cyber security risk. Outlining the fundamentals of risk management and describing techniques you can use to manage cyber security risks.

https://www.ncsc.gov.uk/collection/risk-management-collection

Appendix 3 –
The National Data Guardian reports

The NDG report

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