NHS England

Data Security Standard 1

Personal confidential data

The bigger picture and how the standard fits in

2023/24

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.

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

"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 [redacted] particularly in large organisations. The board as a whole should take responsibility."

NDG Review

Commented [TG1]: Switch to embedded hyperlink to avoid mention of NHS digital

The organisation has a framework in place to support lawfulness, fairness and transparency (1.1)

ICO registration number (1.1.1)

Registering with the Information Commissioner's Office (ICO)

You are required to provide the following details to the ICO for registration:

- organisation type, for example, whether your organisation is a public authority or charity
- name and address of the controller (this will be your organisation's registered address, such as a hospital trust's headquarters, or smaller organisation's registered office address. If you work for a branch of a larger organisation, it will be your parent organisation's registered address)
- any other trading names your organisation has (for example, your registered company name may be "Care Partnership Ltd" but your trading name may be "Maple Homes")
- number of staff members (the options are less than 10, up to 250, or more)
- annual financial turnover. This can be found in your annual accounts which may be published on your website, on Companies House, or you can speak to your finance team
- a relevant person in your 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
- details of your Data Protection Officer, if your organisation is required to have one
- name and contact details of the person completing the registration process

For more information about the ICO, you can visit the ICO website where you can also find further guidance on the data protection fee and start the registration process.

Documenting personal data (1.1.2)

Information register

To be legally compliant with data protection legislation, your organisation must keep a register of all the different types of information it stores, shares and receives. The register should also detail all the digital and physical places where personal and sensitive information is stored, and how your organisation keeps it safe.

Previously, you may have documented the storage of your information within an information asset register (IAR) and the details of sharing of the information in a records of processing activities (ROPA). However, using one combined document will allow all of your processing and storing information to be documented in the same place. A template information assets and flows register (IAFR) produced by NHS England will be is available Transformation Directorate's information governance guidance page

Your register must include your organisation's name and contact details, and the following details for the information held and shared:

For each information asset (a collection of information, grouped by type):

- a description of the data collection (for example, safeguarding referrals database, or occupational health records)
- retention period (these must be compliant with the NHS Records Management Code of Practice. If not covered by the code, it should only be held for as long as it is necessary)
- whether your organisation is the controller or a processor, and where applicable, details of any joint controller (with their contact details, their representative if applicable and their DPO)
- the team, information asset owner and administrator (these could be job roles or named individuals)
- media type (digital or paper)
- the location of the data (this will include specific physical locations, such as "the filing cabinet under the table in reception", and digital locations, such as laptop devices, care planning systems, URLs to where data is stored on a shared drive, or URLs to web hosted platforms)
- geographical location of the data (UK, or specify other country)
- business criticality, which is the importance to your organisation (low, medium, high, critical)
- frequency of update
- frequency of backup
- a description of the technical and organisational security measures in place (for example, encryption at rest, pseudonymisation, locked cabinet, access restricted area, role-based access controls)

For each regular flow of information (sending out or receiving):

- a description of the flow (for example, blood test results, hospital discharge forms)
- the purposes of the flow (for example for individual care, research, payroll)

- whether the flow is coming into your organisation or going out and who is the recipient or sender
- the legal basis for processing under UK GDPR Article 6. This is likely to be

  - 6(1)(b) performance of a contract with the data subject

  - 6(1)(c) legal obligation

  - 6(1)(e) public interest task or

  - 6(1)(f) legitimate interests

- the legal basis for processing special category data if applicable under UK GDPR Article 9. This is likely to be:

  - 9(2)(h) (provision of health and social care and systems)

  - 9(2)(i) (public health) or

  - 9(2)(j) (research)

- categories of individuals (for example, patients, service users, staff)
- categories of data (for example, personal demographic, sensitive financial / HR, health, sensitive health, highly sensitive health)
- the categories of recipients of the personal data (for example all organisations within the Integrated Care System, your organisation's finance team, the police, ambulance services)
- method of transfer (by hand, post, telephone, email, electronic transfer)
- details of any data transfers outside the UK, including a record of the transfer mechanism safeguards in place
- how you comply with the common law duty of confidentiality:

  - implied consent

  - explicit consent

  - approval from the Secretary of State or Health Research Authority following an application to the Confidentiality Advisory Group under section 251 of the National Health Service Act 2006

  - statutory requirement to disclose confidential information which overrides the duty of confidence

  - overriding public interest

  - health and care data is not used so it does not apply
- the format of the data (paper, database, PDF files, video files)
- whether a Data Protection Impact Assessment (DPIA) has been completed
- frequency of data transfer (ad-hoc, daily, monthly, quarterly)
- whether the national data opt-out has been applied to the sharing

- whether a data sharing agreement, data processing agreement, contract or similar is in place, when it ends and where it is located (a URL link to the location in your shared drive may be added, physical location or online data sharing agreement management platform specified)

One-off flows do not need to be added but depending on risk, there may need to be a DPIA (such as for transferring all of your organisation's data from one IT supplier over to another).

The register should have been reviewed and approved by your senior management team (in accordance with your governance structure) at least once in the last year.

For more information about records of processing and the lawful basis please refer to the ICO's guidance, which also includes practical advice and templates.

Transparency information (1.1.3)

What transparency information is

Individuals have a right to be informed about the use of their data. Transparency information is also fundamental to individuals being able to exercise their other rights when you are processing their personal data. This includes your staff, visitors (for example to a hospital or care home) patients and service users including children.

Privacy notice

You must publish transparency information about your organisation's data processing activities which informs people about their rights under data protection legislation and how to exercise them.

This is known as a privacy notice. It should explain:

- your organisation's contact details
- the Data Protection Officer's contact details (if your organisation has one)
- if your organisation is not the Controller, the details of the Controller and their Data Protection Officer
- what personal data you are processing
- the purpose for doing so
- the names or categories of organisation the data will be shared with
- the lawful basis for processing

- a list of rights and how they apply to the processing you are undertaking
- your procedure for subject access requests and other data subject rights requests such as the right to object
- the retention period for the data (in line with the Records Management Code of Practice for health and adult social care organisations. For any data not covered by the Code, it should be held only as long as is necessary)
- that individuals have a right to complain to the ICO

Where applicable to the processing, the following details should also be provided:

- contact details of your representative if you are based outside the EU
- explain what the legitimate interests are if this is your legal basis for processing
- details of data transfers to countries outside the UK and what safeguards are in place to protect the data
- how an individual can withdraw consent if this is your legal basis for processing
- whether there is a legal or contractual obligation to provide your organisation with personal data and what will happen if this is not provided
- whether there is any automated decision making (including profiling) that has a legal or similar effect on individuals. Provide meaningful information about the logic involved and explain the potential effects.

Your organisation must provide privacy information that is:

- concise
- transparent
- intelligible
- clear
- in plain language
- communicated in an effective way

Individuals must be made aware of this information. It can be sent to them directly via correspondence, or indirectly through the use of leaflets, noticeboards and websites, but it must be easily accessible.

You may choose to display different privacy notices for different audiences. For example, one for staff and another for members of the public. You may also choose to display separate privacy notices for separate processing; one for the use of cookies on your website; another for the data you process for providing care; and a further one for data used for national screening programmes.

For more detailed guidance on transparency information, please see the ICO's guidance on the right to be informed. A template privacy notice (PN) produced by NHS England is available on the Transformation Directorate's information governance guidance page.

Hardware and software assets (1.1.4)

Know your assets

This encompasses those assets that hold personal data but also those holding business and commercial information.

Systems for holding personal data

Personal data can be held in systems such as:

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

Keeping a record

There should be a record of software and associated hardware assets and an individual(s) with assigned ownership of protection assets (such as an Information Asset Owner).

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.

Staff with key responsibilities (1.1.5)

There are strict criteria determining who can be appointed into key data protection and data security positions within health and care organisations. It may be that one individual fulfils multiple functions if your organisation is small. This is acceptable as long as it does not introduce a conflict of interest between the roles.

Data Protection Officer (DPO)

It's a legal requirement to appoint a DPO if:

- you are a public authority or body
- your core activities require large scale, regular and systematic monitoring of individuals
- your core activities consist of large scale processing of special categories of data, such as health and care data

There is a tool on the ICO's website to help you understand if you need to appoint a DPO.

The DPO:

- is an independent advisory role held by an expert in data protection
- informs and advises on your data protection obligations, data protection impact assessments (DPIAs) and monitors internal compliance
- acts as a contact point for data subjects and the Information Commissioner's Office (ICO)
- must be adequately resourced and report to the highest management level
- must have sufficiently advanced abilities, as the nature of the health and care information your organisation uses will likely be particularly complex and high risk. In addition, the DPO must understand how relevant legislation and guidance for the health and care sector interacts, particularly the requirements of the common law duty of confidentiality. This may be demonstrated by their experience within health and care, and may be supplemented by professional qualifications in data protection
- must not have a conflict of interest that will prevent them from being able to provide independent advice on data protection. For example, the head of IT would not be an appropriate DPO appointment, as they have an interest in IT projects being approved
- can be an existing employee or externally appointed
- can be a single person shared between groups of smaller organisations

To find out more about DPOs, please see the ICO's website.

Senior Information Risk Owner (SIRO)

The SIRO is a senior advocate for data security and protection matters at board-level.

Their responsibilities include:

- influencing the board to foster a culture that values, protects and uses information for the success of the organisation and benefit of its patients and service users
- staying informed about data security and protection risks, and managing those risks
- signing off key elements of the DSPT
- overseeing the development of information risk policies
- managing high severity cyber alerts and accepting appropriate residual risk
- providing leadership during a major incident or breach
- taking ownership of the organisation's risk assessment processes
- ensuring that the organisation's approach to information risk is communicated to all staff and effective in terms of resource, commitment and execution
- ensuring the organisation's risk policy is implemented consistently by Information Asset Owners (IAOs)

The SIRO should be an Executive Director or other senior member of the board (or of an equivalent senior management group/committee).

The role of SIRO may be assumed by the Chief Information Officer (CIO) if the CIO is on the board, however this would not be best practice.

When cover is needed during times of absence, it is acceptable for another board member to act as SIRO delegate.

However, neither the permanent post nor the temporary delegate position should be assumed by the Caldicott Guardian, as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

For more information about how the SIRO can guide the board towards excellent standards in data security, see the NCSC board toolkit.

Also see 3.4.1 and 3.4.2 for cyber SIRO and board data security and protection training.

Caldicott Guardian

Caldicott Guardians are senior people within organisations that help ensure confidential information about health and social care service users is used ethically, legally, and appropriately.

They ensure that their organisation(s) satisfy the highest ethical and legal standards for processing the confidential information of patients, service users and staff members.

Their responsibilities include advising on disclosures of confidential information (particularly in situations of legal and/or ethical ambiguity), involvement in addressing patient or service user complaints, reviewing and advising on data protection documentation, contributing to audits and helping to investigate data breaches.

It's essential that the Caldicott Guardian is a person with the ability to apply the Caldicott Principles wisely, and has the courage to speak openly and with authority to their organisation's highest level decision makers. All Caldicott Guardians need a strong commitment to the role. They need the inquisitiveness to question, analyse and challenge, and the ability to apply wise judgement to the precise circumstances of each case.

It's preferable for Caldicott Guardians to be experienced health and social care practitioners to facilitate their role as an advocate for patients and service users, and to act as the conscience of the organisation. However, this is not a mandatory requirement.

For smaller organisations where it may be difficult to identify an appropriate individual to perform this role, the Caldicott Guardian function may be provided by another organisation. For example, commissioning organisations might consider supporting smaller organisations. Also, a Caldicott Guardian may provide the role across multiple organisations if appropriate.

It may be appropriate in some organisations for the Caldicott Guardian and DPO roles to be held by the same individual, provided that they have the relevant background, knowledge and experience and that any conflicts of interest are managed openly and appropriately. However, it would not normally be appropriate for the same person to be both SIRO and Caldicott Guardian, due to the possibility of a conflict of interest and the decision-making role that the SIRO may hold.

Further guidance is available on the role, responsibilities and which organisations should appoint a Caldicott Guardian.

Information Governance Leads

Information Governance (IG) Leads are representatives from senior management who co-ordinate and manage the IG work programme.

It's recommended that the roles of DPO and IG Lead are carried out by different people in larger organisations. If the roles are carried out by the same person, there should be no conflict of interest between the duties of the IG Lead and those of the DPO.

The following duties must be carried out, regardless of who assumes the role:

- ensuring effective management, accountability, compliance and assurance for all aspects of IG (data protection/privacy, confidentiality, freedom of information and subject access)
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements
- maintaining the appropriate documentation to demonstrate the organisation's commitment to IG responsibilities and providing direction in formulating, establishing, and promoting IG policies
- ensuring the annual DSPT assessment, associated audit and improvement plan are carried out, documented, approved, and reported in line with the requirements of the NHS Standard Contract
- communicating the approach to information handling to ensure that staff understand the need to support appropriate information sharing
- ensuring that appropriate training is made available to all staff and completed as necessary to support their duties
- ensuring transparency so that the public are aware of how their information is used and shared
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards
- monitoring information handling activities to ensure compliance with law and guidance
- providing a focal point for the resolution and/or discussion of IG issue
- keeping up to date with IG and data security developments

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 IG Lead, or an IT Manager.

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

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

- informing and advising and implementing an organisation's security strategy including the effectiveness of security controls
- monitoring compliance/certification with a range of legislation and standards which could include Network and Information Systems (NIS) Regulations, the security

elements of UK GDPR and the Data Protection Act 2018, Cyber Essentials, ISO 27001 and the Data Security and Protection Toolkit (DSPT) itself

- responding and coordinating the response to high severity alerts and advisories
- responding to and coordinating efforts to security related incidents
- co-operating with NHSEngland , the ICO and National Cyber Security Centre (NCSC)
- being a champion and advocate for good information security practice in the organisation
- ensuring information security mandatory and role-based training is provided to staff

For useful resources for managing a cyber security incident, see our cyber and data security pages.

For industry guidelines see ISO 27001: Understanding Security Roles and Responsibilities and Why They Are Vital to the Success of Your Security Program - risk3sixty.

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

Consent (1.1.6)

Consent under common law

An individual's consent may be implied where their health and care information is shared with the individual's health and care team in order to facilitate the provision of care to the individual. Individuals may withdraw their implied consent under the common law duty of confidentiality. The impact of any decision to withdraw consent must be clearly explained to the individual, bearing in mind that in some circumstances, this will mean they will not be able to be treated.

Where an individual's health and care information is shared or used in ways they would not reasonably expect, their consent under the common law duty of confidentiality may not be implied and you need explicit consent. Consent to share their information with third parties, such as solicitors, friends or family members and unpaid carers must also be sought. Find out about the rules around consent and sharing information with the police.

Where explicit consent is either not possible or if the individual refuses to provide it, the common law duty of confidentiality may be overridden by a legal duty to share information or by an overriding public interest. The overriding public interest must clearly demonstrate that the public interest benefits override the rights of an individual for the use of their information.

Consent may be given verbally or may be written. If consent is verbal, this should be recorded in the individual's health and care record as good practice.

You should have processes in place for the obtaining and withdrawal of consent as necessary. This may be documented in a single confidentiality policy and procedure or within dedicated sections in other documents.

Consent under UK GDPR

Consent is one of a number of legal bases for processing personal data under UK GDPR requirements. However, consent is not usually the legal basis relied on where health and care personal data is processed for individual care or medical research.

An example of where you might rely on UK GDPR consent would be where an individual provides consent for their cookies to be used on websites. If you choose to rely on consent then you must have a process in place for recording consent, which includes an effective audit trail of how and when consent was given by patients for the processing of their data.

In line with ICO guidance, your records must demonstrate:

- **who consented:** the name of the individual, or other identifier (such as an online username)
- **when they consented:** a copy of a dated document, or online records that include a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation
- **what they were told at the time:** a master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy or other privacy information, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time
- **how they consented:** for written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation - it doesn't need to be a full record of the conversation
- whether they have withdrawn consent: and if so, when

You should maintain an ongoing process which allows patients and service users to withdraw consent at any time they choose, and prompts individuals to re-evaluate their consent if the processing changes. Refer to the ICO's guidance for practical advice on how to implement this.

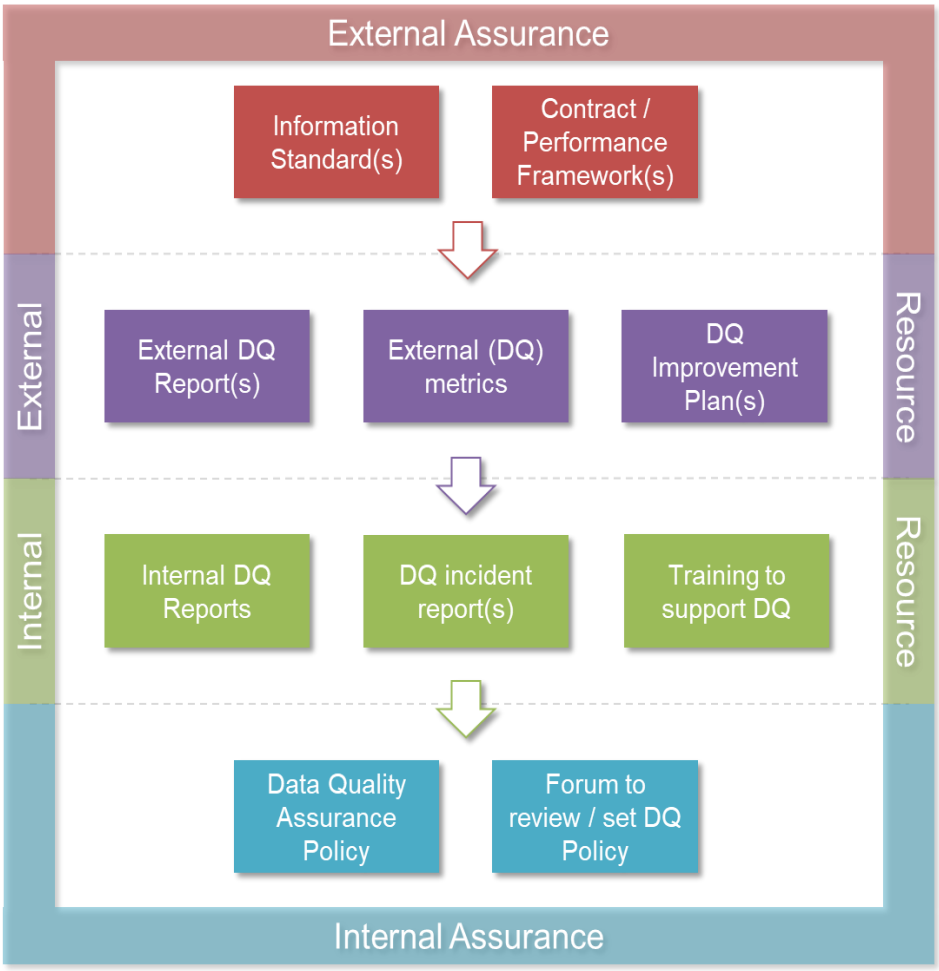
There is no set way for how your record of consent should be stored, but the record should cover the entire consent lifecycle, be auditable and it should also be supported by a policy and procedure.

For further guidance on consent under common law, UK GDPR and the legal implications of processing health and care data, see the NHS Transformation Directorate guidance on consent.

Data quality (1.1.7 and 1.1.8)

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 section.

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 England on the Information Standards web pages 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 conform 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 several 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 England's Data Quality Maturity Index (DQMI) for providers of Mental Health Services. This will be extended across other provider types in 2019/20.

Model Health System - NHS England and Improvement use the DQMI as a metric within the Model Health System series of metrics.

Care Quality Commission (CQC) Well-led Domain - The CQC collects 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 subcontractors and vendors alike

External Data Quality reports and 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 England 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 CDS DQ dashboards published monthly by NHS England 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 England 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 England through the Data Processing Service (DPS) for collections such as Mental Health Services Dataset (MHSDS), Maternity Services Dataset (MSDS) and the Community Services Dataset (CSDS) and Improving Access to Psychological Therapies (IAPT). The Mental Health Data Hub contains a wealth of data quality reports, as does the Community Services Data Quality Dashboard
- 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 England 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 subcommittee/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), 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 data quality 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 DQMI, CDS Data Quality Dashboards and associated key performance indicator (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.

Data quality 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 and 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 policies such as that for information governance or 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:

- **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 and Protection Toolkit
- **measurement of good data quality:** defines what dimensions will be used to measure data quality, such as completeness, validity and integrity
- **validation and quality assurance:** details all the internal and external resources that will be used to assure data quality, such as DQMI, SUS Data Quality Dashboards, submission data quality 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:

- **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, such as information governance group
- **links to other groups:** what other groups or boards it has dependencies on or have dependencies on it within the organisation - for example, 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 data quality reports issued by NHS England (national flows) or Data Services for Commissioners Regional Offices (DSCRO)/commissioning support unit (CSU) (local flows) as appropriate
- **metrics:** monitoring of key performance indicators (KPIs) and other performance related metrics such as the DQMI for underlying data quality issues

- **improvement:** delivering against DQIPs as defined by clinical commissioning groups (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 data quality 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 (1.1.7 - 1.1.8)

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.

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 an 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.

[1] OPCS-4 Classification of Interventions and Procedures Version 4.10 (2023) – 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.

Guidance – Robust Data Quality and Clinical Coding Audit Programme

Introduction

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

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.

[4] Organisation in this context is referring to both NHS and non-NHS organisations responsible for the delivery of patient care.

Audit Programme – Data Quality (Clinical Coding)

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

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 a:

- continuous clinical coding audit programme comprising several smaller audits undertaken throughout the course of the year as part of routine maintenance of standards (see also Clinical Coding Auditor Programme, below)
- single one-off audit, which should be undertaken every 12 months

The number of care professional admitted care episodes (hereafter referred to as ‘episodes’)audited must be a minimum of 200 episodes for Acute Trusts and 50 episodes for Mental Health Trusts. (See also Clinical Coding Auditor Programme, below)

Data Quality (Clinical Coding) Audit Specification

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 (at the time of the audit, not the time the coding was completed; code assignment itself will always be assessed against the national clinical coding standards in place at the time of coding) and be undertaken by a approved clinical coding auditor who has complied with all the requirements of the Terminology and Classifications Delivery Service Clinical Coding Auditor Programme (CCAP) as described in the CCAP Handbook.

Commented [TG2]: Dead link

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.

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

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

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.

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-4.10 reference book, or the National Tariff Chemotherapy Regimen List will not be pursued.

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 (such as 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.

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

A summary of the methodology titled A Guide to Clinical Coding Audit Best Practice is available for reference by anyone who is not an approved clinical coding auditor.

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.

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. A Glossary of Clinical Coding Audit Types is available for reference purposes. The clinical coding auditors have a responsibility to satisfy themselves that the sample is random within this constraint.

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* 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 episodes.

*Beyond this published minimum, each organisation needs to decide a meaningful number of 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.

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.

Trusts must meet or exceed the required percentage across all 4 areas in order to meet the attainment level for a DSPT clinical coding audit.

Individuals' rights are respected and supported (1.2)

Individual rights (1.2.2)

Individual rights under UK GDPR

UK GDPR provides the following rights for individuals:

1. The right to be informed (see evidence item 1.1.3)
2. The right of access (see evidence item 1.2.3 below)
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Your organisation must have a policy and procedures in place documenting how an individual can exercise their rights. This may be captured in a single policy, or it may be separated out, for example you may have a separate subject access request procedure. Instructions for individuals of how to make a request must be made available to them, such as through privacy notices.

The right to rectification

People have a right to rectification if you hold inaccurate factual information about them. Depending on the purposes of processing, people also have a right to have incomplete personal data completed. Holding inaccurate information would likely be a breach of UK GDPR. However, care needs to be taken when amending any information from health and care records. This is because it may have been viewed and relied upon for a decision. The IG portal contains further guidance on amending patient and service user records.

The right to erasure

The right to erasure allows an individual to request removal or deletion of personal data. This right only applies in certain circumstances. You can refuse to comply with a request for erasure of personal data if processing is necessary:

- to comply with a legal obligation
- to perform a task in the public interest
- for individual health and care purposes
- for reasons of public health
- where erasure is likely to seriously impair or prevent scientific research from achieving its objectives

For more information on where the right to erasure does not apply, please refer to the ICO guidance.

These are legal bases for most processing in health and care so it is unlikely that the right to erasure will apply to health and care records. An example of where it may apply is if an individual supplies details of their circumstances, such as their patient story, to be used as promotional material. The individual may change their mind and ask for you to delete the information you have been provided. It is important to note that if the information has already been published online, although your organisation can remove copies it holds and will make reasonable efforts to request the same of other controllers processing the data (such as social media providers), the nature of the internet is that a copy may persist elsewhere. This should be made clear to the individual at the point they provide consent for you to use their story.

The right to data portability

The right to data portability allows people to obtain and reuse their data across different services, for example from one IT system or application to another.

The right only applies if the personal data has been provided by the individual, where the lawful basis under UK GDPR is either consent or for a contract with the data subject, and the processing is by automated means. This right is therefore mainly likely to apply to organisations providing services directly to patients and service users through an app or online platform. Information must be provided within a month.

The right to object

In certain circumstances, UK GDPR gives individuals the right to object to the processing of their personal data. Your organisation must have procedures and processes in place which ensure that when individuals make objections to processing, they are duly considered and responded to. The right to object applies to situations where you process data for:

- the performance of a task carried out in the public interest), or
- your or a third party's legitimate interests

For direct marketing purposes, the right to object is absolute. Where data is processed for scientific or historical research, or statistical purposes, the right to object is more limited.

It is unlikely that an objection would be upheld where the data is processed for individual care, but each request must be considered on a case-by-case basis. However, it is important to note that there are other routes in which an individual can raise an objection to processing.

Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision solely based on automated processing that results in a legal effect on them or significantly affects them in some other way, such as in the way they receive care. UK GDPR defines 'profiling' as any form of automated processing of personal data to evaluate certain personal aspects of an individual, especially to analyse or predict certain things, including health.

An example of where this could happen in some sectors is AI. However, at the moment health and care professionals usually make the final decision as set out in the AI guidance on the IG Portal. Similarly, data used for risk stratification purposes are likely to be subject to review for a decision by a human health and care professional and so this is not considered automated decision making.

Subject access requests (1.2.3)

UK GDPR gives individuals the right of access to their personal data from any health and care organisation that holds records on them. This right is commonly referred to as a 'subject access request' (SAR).

You must ensure that your organisation has a procedure that allows individuals to be provided with a copy of the data where requested, along with information about the processing.

For practical guidance on responding to SARs, including the procedures you must follow, the necessary timescales, and the situations in which they can be refused, see guidance on the IG Portal.

It should be noted that organisations are no longer required to submit FOI information for the purposes of the DSPT, however this does not negate or diminish required organisation obligations. For more information, see the ICO's guide to freedom of information.

National data opt-out (1.2.4)

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of data that identifies them for research or planning purposes.

This does not apply to anonymous data, such as statistics of how many people received a specific treatment. You must ensure that you have a mechanism to apply any opt out decisions to relevant datasets. Find out detailed information about how to implement the national data opt-out.

Accountability and governance in place for data protection and data security (1.3)

Data security and protection policies (1.3.1)

You must provide evidence that your organisation has data security and information governance (IG) policies in place. As a minimum, your policies should cover:

- data protection and confidentiality, including: data protection by design, data protection impact assessment, transparency and data subject rights
- Freedom of Information and Environmental Information Regulations (if applicable)
- data security
- records management
- acceptable use of IT
- data quality
- re-use of public sector information (if applicable)
- arrangements for any of your staff members who work from home such as remote working policies, network access, video conferencing

The size and complexity of your organisation will determine your approach. An all-encompassing policy might be sufficient in smaller organisations, whereas larger organisations may require multiple policies supported by standards and procedures.

The policies should be board approved. The process for this will depend on your organisation's governance structure. For example, the policies may be sponsored at board level by the senior information risk owner (SIRO), and ratified at a steering group with delegated authority. Alternatively, in a smaller organisation, the policy may be approved by the IG lead and ratified by the senior management team, with representation from the board. It is important the policies are effective, acknowledged and understood.

In addition, your policies should:

- be reviewed at regular intervals
- be your 'live' policies and finalised (not draft)
- be version controlled
- detail the last and next review date, which should not be exceeded
- provide an explanation for why they have not been updated in the last three years, where this is the case

- link to other corporate policies where appropriate (such as an acceptable use for IT policy linking to a disciplinary policy)
- be available to staff and the public

Compliance with policies and procedures (1.3.2)

Assigning responsibility

The responsibility for monitoring and auditing access to confidential information should be assigned to an appropriate staff member, such as the Caldicott Guardian, IG lead or equivalent.

This member of staff is responsible for ensuring that confidentiality audit procedures are developed and communicated to all staff who can access confidential 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

Spot checks

Your organisation should undertake spot checks to ensure that your staff understand and adhere to policies and procedures on data protection. Examples of events that you should audit for frequency, circumstances and location for example, are:

- failed attempts to access confidential information
- repeated attempts to access confidential information
- attempts to access confidential information from outside the system, particularly from overseas locations (where technically feasible)
- successful access of confidential information by unauthorised persons
- evidence of shared login sessions/passwords
- disciplinary actions taken
- devices are locked when not in use
- cupboards and areas with confidential data are locked and access is restricted
- confidential waste is disposed of appropriately (shredded or put into confidential waste bins)

Development and improvement

The feedback you learn from staff awareness audits, inductions and spot checks should be used to refine your procedures and further raise staff awareness of key issues around confidential information.

SIRO responsibility (1.3.3)

You should have a board-level individual who has overall accountability for the security of networks, information systems and IG and drives regular discussion at board-level. They should be the board champion on data security and protection matters. Their responsibilities as SIRO should be included in their job description and responsibilities document.

See section 1.1.5 for more information about the responsibilities and role of the SIRO.

Lines of responsibility and accountability (1.3.4)

You should be able to evidence clear lines of accountability and responsibility between your organisation's named individuals for data security and data protection. The lines should be transparent, well-defined and documented.

An example of how this could work is shown below:

Board:

- SIRO
- Caldicott Guardian

Information Assurance Group:

- Head of IT (accountable to SIRO)
- IS/Cyber Manager (accountable to Head of IT)
- DPO or IG Lead (accountable to Caldicott Guardian)

Information Assurance Working Party:

- Cyber apprentice (accountable to IS/Cyber Manager
- FOI Lead (accountable to DPO or IG Lead)

Data security risk register (1.3.5)

Risk management should be a key component of your organisation's data security and protection framework. It should be treated as a continuous cycle. Your organisation should hold two levels of risk register:

DSP risk/unit register

- Either one central dedicated data security and protection risk register or multiple registers should exist at the level of your organisation's units/locations.
- Depending on your risk framework, you may hold a separate IT risk register or it may be included in the DSP risk register.
- In accordance with your risk framework, it may be that where a DSP risk is also a corporate level risk, that you will need to record it on both registers so there is oversight at both levels.

Corporate risk register

- For your organisation's corporate-level risks.
- Risks on the DSP risk/unit register should be escalated to the corporate risk register when they exceed your organisational threshold and interact with corporate risks. This should be done in line with your organisation's risk appetite, which should be approved by the board.
- Risks on the corporate risk register should be de-escalated to the DSP risk/unit register if the risk level is sufficiently reduced (such as by new controls being put in place or systems being updated)

There is not a single adopted information security risk management framework mandated by the Data Security and Protection Toolkit. However, the framework adopted by your organisation should be a recognised and acceptable information security risk management framework that covers both cyber security and IG aspects.

Some of the more common frameworks are detailed in The National Cyber Security Centre (NCSC) risk management collection.

Top priority risks (1.3.6)

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

For example, for 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 city, 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 of resources either financial or staff.

Whatever your top three risks are, they should be discussed by the leaders of your organisation, who should put plans in place to mitigate and reduce them. 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). This may be achieved by discussing the risks at your information assurance group or equivalent, with outcomes and actions reported into the board by the SIRO, who will sit on both the information assurance group and the board. Alternatively, it may be reported to the board as part of a regular (at least annual) SIRO-sponsored written report on IG and cyber activities and risks. Actions and information arising from this should be cascaded to all management levels as appropriate.

Access controls (1.3.7)

As set out by the Information Commissioner's Office (ICO):

> The UK General Data Protection Regulation (UK GDPR) requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is ‘data protection by design and by default’.
>
> In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.

Data access

It is important that staff are only allowed to see, access, modify and delete data if their job requires them to do it. There are generally two ways of achieving this: technical controls and physical access controls.

Technical controls

Technical controls can include, but are not limited to:

Individual user logins: staff have their own logins to systems to allow effective auditing and access controls. Shared logins, including admin accounts not tied to one individual make it difficult to identify inappropriate access and to restrict access efficiently.

Role-based access: staff only have access to relevant information required for their roles. This may be achieved by granting folder or file access to a limited number of staff.

Smartcard enabled access: smartcards and other forms of physical certification are used as an extra authentication factor for accessing systems.

Two factor authentication (2FA): staff must confirm their identity via an additional method, such as the use of a password and a code received by text message to their registered device.

Encryption: data is encrypted. This includes data that is stored and data being transferred.

Endpoint port control: access to USB (and other ports) is controlled, restricting who is able to use them and what data they are permitted to copy. This is particularly important on end points.

Pseudonymisation/anonymisation techniques: anonymised or pseudonymised datasets are used whenever possible.

Using test data: data that is completely unrelated to live data is used in situations such as training, where real data is not needed.

Data loss prevention: a system that inspects data going outside the organisation and can report or block it.

Control of personal web-based email systems: access to web-based mail is controlled to protect against the use of commercial web-based email systems which upload corporate data in a way which is not secure.

Effective audit logging: audit logging and monitoring is used as a deterrent to inappropriate use and helps inform development of new technical controls.

Physical controls

Physical controls can include, but are not limited to:

- lockable doors, windows and cupboards
- privacy screens
- dedicated spaces to have confidential conversations
- sound-proofing of meeting rooms
- clear desk procedures
- identification IDs
- key card access
- code locks for secure areas

Data protection impact assessment (1.3.8)

A data protection impact assessment (DPIA) is a process which has been designed to help you systematically analyse, identify and minimise the data protection risks of specific projects or plans within your organisation.

An effective DPIA will help you assess and demonstrate compliance with your data protection obligations. Additionally, it will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

When you should conduct a DPIA

You must legally do a DPIA before you begin any type of processing which is “likely to result in a high risk to the rights and freedoms” of individuals. This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects
- process special category data on a large scale, such as health and care information
- systematically monitor publicly accessible places on a large scale (such as CCTV)

More specifically, situations in which you must undertake a DPIA include when your organisation is planning to:

- use new technologies, such as remote monitoring, or a new care planning tool
- use profiling or special category data to decide on access to services, such as for risk stratification or for eligibility screening tools
- profile individuals on a large scale, such as for risk stratification and some types of population health management
- process biometric data, such as to use fingerprint or facial recognition to allow access to an app
- process genetic data, such as using DNA sequencing to predict rare disease risk
- match data or combine datasets from different sources, such as combining GP and social care data to build up a fuller picture of vulnerable individuals
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing'), such as for health and care system planning
- track individuals' location or behaviour, such as for a food logging and exercising app
- profile children or target marketing or online services at them, such as apps or websites to support children with their mental health
- process data that might endanger the individual's physical health or safety in the event of a security breach, such as for data relating to domestic violence and safeguarding

It is, however, best practice to conduct a DPIA for all processing, as the process will enable you to identify whether the processing is actually high risk or not. This may result in you only conducting the screening question process, but it is necessary so that you can justify your decision not to complete a full DPIA.

How to conduct a DPIA

Before and during the DPIA process, you should consult with your data protection officer (DPO) or IG Lead. The process should be agreed and signed-off at board or equivalent level. The steps in a typical process for a DPIA which is compatible with ICO guidelines is stated below:

1. Identify need for a DPIA
2. Describe how the data will be used, shared and stored
3. Consider consultation
4. Ensure your proposed use is necessary and only uses relevant data
5. Identify and assess risks
6. Identify measures to mitigate the risks
7. Sign off and record outcomes

8. Integrate outcomes into plan
9. Keep under review

For practical guidance on each of the steps described above, please refer to the ICO's guidance on how to do a DPIA. A template data protection impact assessment (DPIA) produced by NHS England is available on the Transformation Directorate's information governance guidance page

Processing likely to result in high risk

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. The ICO has stated that written advice will be provided within eight weeks, or 14 weeks in complex cases.

For examples of processing likely to result in high risk, see the ICO's guidance on processing 'likely to result in high risk'.

Transparency

It is good practice to publish DPIAs, particularly those for which there is a significant public interest. A DPIA will make it easier for people to understand how and why you are using their information. It can also reassure people that you are protecting their interests and meeting their expectations of privacy.

You should redact any commercial, personal or sensitive information that may lead to a security risk before publishing a DPIA. Alternatively, you may wish to publish a summary of the DPIA.

Direction of organisational practices for data security and protection (1.3.9)

The board should provide direction on data security and data protection, which should then be disseminated throughout the organisation through its policies, projects and procedures.

Example scenario

How this might be practically applied:

Problem identified by the board:

- Risk of phishing attacks through staff members' emails.

Actions for the board:

- The board launches an awareness campaign, sponsored by the SIRO

Actions for the information assurance group:

- The information assurance group ratifies the awareness campaign, agreeing actions to be completed

- Information security/cyber manager implements a simulated phishing exercise

Actions for the information assurance working party:

- Cyber apprentice compiles suspicious email reports on a weekly basis for submission to the information security/cyber manager

The results of the campaign will then be fed into the information assurance group for review, with outcomes and any further recommendations filtered by to the board through the SIRO, who also attends (or chairs) the information assurance group.

For more information on how to establish standards for accountability in your organisation, please refer to the ICO's Accountability Framework.

Records are maintained appropriately (1.4)

You must have a records management policy in place.

The Records Management Code of Practice 2021 will support you in developing a policy and managing records appropriately. It provides a framework for consistent and effective records management based on established standards. It covers organisations working within, or under contract to the NHS in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities.

Data disposal

It is important to note that data destruction can be physical (such as shredding) and digital (secure deletion). Your data disposal contracts and suppliers should reference or include guidance on disposal of electronic media containing personal or sensitive data. For further information including on the standards for secure deletion, please refer to the National Cyber Security Centre guidance.

Traditionally, paper-based disposal has consisted of simple vertical shredding. However, this method is not suitable for sensitive or confidential information. BS EN 15713:2009 and the HMG Information Assurance Standard (IS5) requires the shredding of sensitive paper records to be conducted using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm.

If your organisation uses third parties to dispose of (destroy by any means, including incineration) or archive personal data, there should be a contract in place which requires the third party to have appropriate security measures in place in compliance with data protection law.

The nature of the devices you are disposing of, and the devices themselves (such as paper, hard drives, USB memory sticks, CDs), will change over the course of your contract with a supplier. You therefore need to review contracts with suppliers periodically.

The contract with the supplier should also contain a provision allowing you, or a contracted third party auditor, to periodically audit them. 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 referenced
- 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

Your third-party supplier should record each item that has been disposed of on a destruction certificate. This can be one certificate per item, or multiple items on one certification. It is important that these items are known and can be referenced individually.

A destruction certificate with the following line item is not acceptable given that items have not been referenced individually and they are untraceable:

- 50 x SATA mixed sized hard drive destroyed

Whereas a destruction certificate such as the below, where items are individually referenced and the disposal method is specified, would be 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

Appendix 1 - Useful resources

Information Governance Panel Guidance: NHS England Transformation Directorate – A portal of guidance on numerous key IG topics which has been reviewed by the Health and Care Information Governance Panel, including the Information Commissioner's Office (ICO) and the National Data Guardian (NDG).
Information governance guidance - Information governance - NHS Transformation Directorate (england.nhs.uk)

Records Management Code of Practice 2021: NHS England Transformation Directorate - The Records Management Code of Practice for Health and Social Care 2021 is a guide for you to use in relation to the practice of managing records. It is relevant to organisations working within, or under contract to, the NHS in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities.
https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

Confidentiality Advisory Group (CAG) information: Health Research Authority – Information about the CAG, an independent body which provides expert advice on the use of confidential patient information for research uses, including how to apply and a register for approved applications.
https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/

Caldicott Guardian FAQs: UK Caldicott Guardian Council – Frequently asked questions about the appointment of Caldicott Guardians, their role and responsibilities.
https://www.ukcgc.uk/ndg-guidance-faqs

Guidance on the appointment of Caldicott Guardians, their role and responsibilities: National Data Guardian - Issued under the National Data Guardian's statutory powers, this guidance is about the appointment, role and responsibilities of Caldicott Guardians.
https://www.gov.uk/government/publications/national-data-guardian-guidance-on-the-appointment-of-caldicott-guardians-their-role-and-responsibilities

National data opt-out: NHS England – A service that allows patients to opt out of their confidential patient information being used for research and planning.
https://digital.nhs.uk/services/national-data-opt-out

Guide to the UK General Data Protection Regulation (UK GDPR): Information Commissioner's Office - The Guide to the UK GDPR explains the provisions of the UK GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

FOI self-assessment toolkit: Information Commissioner's Office - The toolkit is designed to help public authorities assess their current FOI performance and provide indicators of where efforts should be focused in order to improve. It also provides templates for taking improvement actions.
https://ico.org.uk/for-organisations/foi-self-assessment-toolkit/

Data protection self assessment: Information Commissioner's Office - This self assessment toolkit will help assess your compliance with data protection law and find out what you need to do to make sure you are keeping people's personal data secure.
https://ico.org.uk/for-organisations/accountability-framework/

Accountability Framework: Information Commissioner's Office - The framework is an opportunity for you to assess your organisation's accountability – one of the key principles in data protection law.
https://ico.org.uk/for-organisations/accountability-framework/

Publications and Resources page on Delen: NHS England - Clinical Coding section on Delen. The information sharing and collaboration platform for users of our Terminology and Classifications products. Here you can access up-to-date information, resources, educational materials and technical support relating to our core products.

Publications & Resources - Delen: Home - NHS England (kahootz.com)
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

Board toolkit: National Cyber Security Centre - Resources designed to encourage essential cyber security discussions between the Board and their technical experts.
https://www.ncsc.gov.uk/collection/board-toolkit

Secure sanitisation of storage media: National Cyber Security Centre - Why sanitisation is necessary, the risks to manage, and how to sanitise affordably.
https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

Appendix 2 – 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

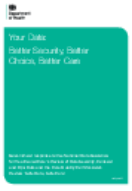
The government response

‘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