group policies and procedures

# data quality policy

|  |  |
| --- | --- |
| Category | Corporate Governance |
| Author | Castleman Healthcare Ltd |
| Responsible Director | Fiona Pickering |
| Date of issue | September 2016 |
| Next review date | September 2025 |
| Document ref & version | Data Quality Policy V1 |

**Related policies and guidance**

**Document revision and approval history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approved by | Comments |
| Final | Sep 2016 |  |  |  |
|  | Apr 2018 |  |  | Reviewed by JL |
|  | Dec 2018 |  |  | Reviewed by JL |
|  | Aug 2019 |  |  | Reviewed by JL |
|  | Sep 2021 |  |  | Reviewed FP and JL |
|  | Sep 2023 |  |  | Reviewed and updated FP |

# Introduction

Castleman Healthcare Ltd recognises that all its decisions, whether clinical, managerial or financial need to be based on information which is of the highest quality. All this information is derived from individual data items which are collected from a number of sources either on paper, or more increasingly, on electronic systems.

Data quality is crucial, and the availability of complete, accurate and timely data is important in supporting patient care, integrated governance, management and service agreements for healthcare planning and accountability.

# Scope

This policy is intended to cover all data entered onto computerised or paper systems. It applies to all clinical and non-clinical data.

This policy is designed to ensure that the concept and importance of data quality to Castleman Healthcare Ltd is disseminated to all staff. It will describe the meaning of data quality, who is responsible for its maintenance and how it can continue to improve in the future.

This policy applies to those members of staff who are directly employed by Castleman Healthcare Ltd and for whom the Organisation has legal responsibility.

# Definition of Data Quality

Data quality is a measure of the degree of usefulness of the data for a specific purpose. Data needs to be:

1. Complete (in terms of having been captured in full).
2. Accurate (the proximity of the figures to the exact or true values).
3. Relevant (the degree to which the data meets current and potential user’s needs).
4. Accessible (data must be retrievable to be used and to assess its quality).
5. Timely (recorded and available as soon after the event as possible).
6. Valid (within an agreed format which conforms to recognised national standards).
7. Defined (understood by all staff who need to know and reflected in procedural documents).
8. Appropriately sought (in terms of being collected or checked only once during an episode).
9. Appropriately recorded (in both paper and electronic records).

# Core principles

As with other Organisations, Castleman Healthcare Ltd will be required by Connecting for Health to achieve certain levels for Data Quality as set out in the Information Governance Toolkit.

The Data Protection Act 1998 requires that information is accurate and up to date. <http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1>. It is vital to observe the 8 principles of the Data Protection Act 1998 – please see appendix 1.

Data quality is a key part of any information system that exists within the Organisations structure. All staff members will be in contact at some time with some form of information system, whether paper or electronically based. As a result, all staff members are responsible for implementing and maintaining data quality and are obligated to maintain accurate records legally (Data Protection Act 1998), contractually (contract of employment) and ethically (professional code of practice).

There will be identified individuals within the Organisation with responsibility for data quality issues (e.g., informatics, data protection/Caldicott). Their specific responsibility will be explicitly stated in their job descriptions.

Responsibilities concerning data quality will be explicitly stated in the job descriptions of staff involved in the collection or processing of data that is input to information systems.

Responsibility for the strategic management of data quality in the Organisation will lie with the Governance director.

Responsibility for the operational management of data quality will lie with the Director of Governance.

The importance of achieving good data quality will be addressed with all relevant staff as part of the induction process at commencement of their employment and they will be expected to complete an online training module.

All data collection and input processes will have an audit trail and any training and development needs will be addressed.

All users will be made aware of their individual and the Organisation’s corporate responsibility for confidentiality and security of data through the Organisations relevant policies and training.

# Importance of Data Quality

Quality information is essential for:

1. Patient care – to deliver effective, relevant and timely care, and minimise clinical risk.
2. Efficient administrative and clinical processes, such as communication with patients, their families and other carers involved in the patient’s treatment.
3. Management and strategic planning, requiring accurate data about the volume and type of previous patient activity and the population health needs to provide appropriate allocation of resources and future service delivery.
4. Establishing acceptable service agreements for healthcare provision.
5. Clinical governance, which depends on detailed, accurate patient data for the identification of areas where clinical care could be improved.
6. Providing information for other Organisations – healthcare commissioners depend on the patient data we send them and need to have confidence in its quality.
7. Being able to benchmark Castleman Healthcare Ltd against other organisations and the National picture.
8. To facilitate and maintain the accurate flow of information between Castleman Healthcare Ltd and external agencies.

# NHS Number

An NHS number is the only unique way of identifying patients in the NHS system. With this in mind, it is imperative that this be recorded correctly and in all systems, where patient information is present.

The NHS number is fundamental to the Connecting for Health National Programme for Information Technology (IT) as it is the common unique identifier that makes it possible to share patient information across the whole of the NHS safely, efficiently and accurately. The NHS number is the key to unlock services such as NHS Care Records Services, eRS (the electronic referral system) and EPS (the Electronic Prescription Service.)

Every NHS patient is issued an NHS number either at birth (England and Wales) or when they join the NHS by registering with a GP practice. It is a unique 10-digit number where the first 9 are the identifiers and the tenth is a check digit used to confirm the number’s validity.

It is the patient’s unique NHS number that will allow the NHS staff to quickly and efficiently locate the correct health care records on the NHS CRS.

On 18/09/2008, the National Patient Safety Agency (NPSA) together with organisations in England and Wales recommending that they use the NHS Number as the national unique patient identifier.

# Validation of Data

**Importance of Validation**

Validation encompasses the processes that are required to ensure that the information being recorded is of good quality. These processes deal with data that is being added continuously and also can be used on historical data to improve its quality.

It is imperative that regular validation processes be undertaken on data being recorded to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include checking for duplicate data, validating waiting lists, ensuring that national definitional and coding standards are adopted and that the NHS number is used and validated.

**Validation Methods**

Validation should be accomplished using either of the following methods:

1. Bulk reporting which involves a large single process of data analysis to identify all areas where quality issues exist and correct them.
2. Regular spot checks, which involves data analysis on a random selection of records against, source material if available. The number of records examined, and the frequency of these checks should be agreed within Castleman Healthcare Ltd.
3. Bulk reporting can be used as an initial data quality tool as this will quickly highlight any areas of concern, however further investigation will be required to identify more specific issues. Spot checks must be done on an ongoing regular basis to ensure the continuation of data quality. Castleman Healthcare Ltd will work towards developing a process for external audits to be undertaken annually in addition to the internal audits, where appropriate.

**Data Standards**

The use of data standards within systems can greatly improve data quality. These can be incorporated into systems either using electronic selection lists within computer systems or manually generated lists for services that do not yet have computer facilities. Either method requires the list to be generated from national or locally agreed definitions and must be controlled, maintained and updated in accordance with any variations that may occur. Any documentation that refers to the data standards must also be updated as needed and disseminated to all relevant parties.

Providers of data must also ensure that they are able to comply with data accreditation, health records accreditation when applicable and undertake routine data quality audit and quality monitoring.

Data quality is an essential part of the overall information governance (IG) framework and is a requirement of the IG toolkit for all data providers.

The legislative framework within which data standards should comply includes:

1. Data Protection Act 1998.
2. Freedom of Information Act 2000.
3. Human Rights Act 1998.
4. Access to Health Records Act 1990.
5. Computer Misuse Act 1990.
6. National Health Services Act 1977.

**Involving Clinical Staff**

Clinicians must be involved in validating data that may have been entered into the system by clinical coding staff. This may involve the clinician manually reviewing the data that has been entered to confirm its integrity. Regular spot checks will help to ensure that discrepancies are minimised. Clinical input should be sought in situations where the data to be amended is held within medical records. In the case of auditable clinical software, suitable amendments should be made, and the necessary explanation recorded on the system.

**External Sources of Data**

The validation process would use accredited external sources of information, for example, the National Strategic Tracing Service to check NHS number, GP etc.

Data pertaining to Secondary Uses Services (SUS), Payment By Results (PBR) and Commissioning coming from external providers and/or information services (including the Health Informatics Service [HIS] and Commissioning Business Support Agency [CBSA]) should have their own data quality policies which are required to meet national standards. The same is valid for third party data/information, e.g., Social Services.

**Source Data**

Staff involved with recording data need to ensure that it is performed in a timely manner and that the details being recorded are checked with the source at every opportunity. The Organisation strongly supports patient involvement and this could be by cross-checking with patient records or by asking the patients themselves.

**Synchronising Information Systems**

In situations where data is shared between systems it is imperative that the source data be validated initially. Any modifications made to this data must be shared with other related systems ensuring there are no inconsistencies between them. These systems must then be examined and authenticated in turn. Continuous synchronisation between systems is required to guarantee that all data sources reflect the same information.

**Timescales for Validation**

Where inconsistencies are identified these must be acted upon in a timely fashion and documented. Locally agreed deadlines will apply to the required corrections, but all amendments should be made within a maximum of two months from the identifications date.

Note: Under the Data Protection Act 1998 (Subject Access), patients are entitled to have their own version of events included in their health records.

# Training and Communication

**Training**

Training is necessary to ensure the relevant members of staff have the appropriate understanding in order to satisfy the Information governance agenda. With suitable guidance, data quality processes will be improved as information will be collected and recorded correctly at the point of entry. This then reduces the requirement for lengthy validation procedures at later dates.

Line managers are responsible for identifying the training requirements of their staff and working with training providers to ensure these needs are met. Staff must be enabled to attend the appropriate training courses allowing them an adequate level of proficiency in order to carry out their functions effectively.

It is vital that all staff working with clinical and business information have received training on data quality and understand the importance it commands within the NHS both for the management and provision of patient care.

**Communication**

Copies of this policy will be made available to staff via the policy distribution process.

# Performing a data quality audit

**Auditing Corporate Records**

As part of the information lifecycle management strategy, an audit of corporate records has been undertaken.

**Guidance Introduction**

1. Corporate information refers to information generated by an organisation other than clinical or care information (service user records). The term describes the records generated by an organisation’s business activities, and therefore will include records from the following (and other) corporate areas:

• Estates/Engineering.

• Financial.

• Information Management & Technology (IM&T).

• Personnel/Human Resources.

• Purchasing/Supplies.

• Information Department.

• Complaints.

**Purpose of the Records and Information Audit**

2. Organisations should carry out an audit of corporate records and information, to establish:

• the type of records currently held.

• the form in which they are held.

• the record keeping systems currently in use, how effective they are and those that need to be developed/updated/procured.

3. Organisations should ensure that current corporate records and closed/archived records are surveyed. The audit should include paper and electronic records collections, for example, records in filing cabinets, storage rooms, databases, web sites and shared network filing areas.

4. A records audit should enable the organisation to:

• ensure corporate record retention periods are in line with the Records Management: NHS Code of Practice - available from the Knowledge Base Resources.

• identify the location of records to assist the organisation to respond promptly to Freedom of Information requests - see requirement 603.

• determine the use made of each category of corporate record.

• determine whether duplicate records exist.

• determine whether it is necessary to retain the record

• assess current and future records storage requirements.

• identify record creation and disposal concerns.

• identify the department responsible for creation, use and management of each record collection.

• create an information asset register.

• identify any information security concerns.

**Corporate Records**

Documented and implemented procedures are in place for the effective management of corporate records.

**Guidance for Corporate Records Management**

1. The records management function should be recognised as a specific corporate responsibility for all organisations and departments providing health, care and advisory services to NHS patients and/or service users. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. It should have clearly defined responsibilities and objectives, and adequate resources to achieve them.
2. In the context of Corporate Information Assurance, corporate information refers to information generated and received by an organisation other than clinical/care (or service user) information. The term describes the records generated by an organisation’s business activities, and therefore will include records from the following (and other) areas of the organisation:

• Estates/Engineering.

* 1. • Financial.
  2. • Information Management & Technology (IM&T).
  3. • Personnel/Human Resources.
  4. • Purchasing/Supplies.

1. This requirement aims to ensure that corporate records, whether paper or electronic, are accessible and retrievable when and where required. It is not only concerned with corporate records that are part of a formal document and record management system but includes any records on network drives and in shared folders. Emails and attachments, and web pages on internet and intranet sites that are considered corporate records, must also be included within the procedures.
2. When handling any type of record, it is important to make the distinction between a record and a document. In the context of this IG Toolkit requirement, a document becomes a record when it has been finalised and become part of an organisation’s corporate information. At this point, the record should not be amended (unless part of records review processes where the version number is also updated) and should only be held in the corporate system, for example, the network drive, shared folder, and not on a local drive on a PC or laptop.

\*\*This requirement should be reviewed in conjunction with requirement 400 (and requirement 440 depending on organisation-type) regarding an Information Quality and Records Management Assurance framework. It should also be reviewed with requirement 604, as organisations may need to undertake a corporate records audit prior to developing record management procedures to ensure they are aware of all the records held, their location and format, which should in turn inform the decisions made to utilise effective records management systems.\*\*

**Records Management – Procedures**

Organisations should ensure they have documented corporate records management procedures in place which are communicated to all staff and set out following areas:

**a. Creation**

i. Record creation is one of the most important processes in records management and organisations should aim to create good records in an effective system. However, creating a record is not enough unless the record is then captured or filed into a filing system created and managed by the organisation.

ii. It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they are not classified or if they are classified inappropriately. Records captured or filed in a corporate filing system will possess some of the necessary characteristics to be regarded as authentic and reliable. Whatever the format of the records, they should be saved into a proper records management system.

iii. A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily.

iv. The documented procedures should inform staff how to create corporate records in a common format, including:

• the difference between a document and a record.

• the referencing to be applied to new records.

• the version control standards to be followed.

• the agreed naming conventions in use in the organisation.

• where an original record should be filed.

• how to apply a protective mark to a record, if appropriate.

**b. Naming**

i. Naming conventions should:

• give a unique name to each record.

• give a meaningful name which closely reflects the records contents.

• express elements of the name in a structured and predictable order.

• locate the most specific information at the beginning of the name and the most general at the end.

• give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

**c. Filing structure**

i. A clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing. Filing of the primary corporate record to local drives on PCs and laptops should be strongly discouraged.

ii. The agreed filing structure should also help with the management of the retention and disposal of records – see **paragraph 5f** below.

**d. File/Folder Referencing**

i. A referencing system should be used that meets the organisation’s business needs and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric; keyword. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, for example, HR for Human Resources, followed by a unique number for each record or document created by the HR function.

ii. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

**e. Tracking and Tracing**

i. There should be tracking and tracing procedures in place that enable the movement and location of records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from or returned to its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

• the item reference number or identifier.

• a description of the item (for example the file title).

• the person, position or operational area having possession of the item.

• the date of movement.

• location cards.

• index cards.

• docket books.

• diary cards.

• transfer or transit slips.

• bar-coding.

• computer databases (electronic document management systems).

• regular record audits.

ii. The system adopted should maintain control of the issue of records, the transfer of records between persons or operational areas, and return of records to their home location for storage. The simple marking of file jackets to indicate to whom the file is being sent is not in itself a sufficient safeguard against files going astray.

**f. Retention and disposal**

Each organisation should have a retention/disposal procedure that is based on the retention schedules contained in the Records Management: NHS Code of Practice. Schedules should be arranged based on series or collections of records and should indicate the appropriate disposal action for all records once the period indicated in the Code has lapsed. Exceptionally, organisations may retain records for longer than the period in the Code where there is a business need to do so, and this is mandated in published local retention policies. These should be agreed with The National Archives if retention is for a period longer than 30 years (currently being reduced to a 20 year period).

In some cases, the appropriate disposal action will be transfer of the records to The National Archives or more usually a Place of Deposit appointed under the Public Records Act 1958 rather than destruction. This alternative should be adopted for those classes of record indicated in the Code ('see Note 1') or in accordance with a local policy agreed with The National Archives or the relevant Place of Deposit appointed under the Act. Such records should be transferred to the Place of Deposit (see Annex E of the Code, or the current listings and contact details on The National Archives website) no later than 30 years (or the current transitional period) from creation of the record, as required by the Public Records Act. Transfers should be made in accordance with policies and procedures agreed in advance with the Place of Deposit.

**Tracking mechanisms to be used should include:**

Systems for monitoring the physical movement of records, for example:

i. When developing or purchasing a records management system, organisations should consider how retention/disposal periods will work or can be factored into the system. For paper corporate records, this may be using clearly marked labels on each folder to state the minimum retention period, and a log kept so that records can be easily appraised.

ii. Electronic document management systems may have the functionality built within them to set the disposal period for a record based on certain defined rules.

iii. Methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.

iv. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

**Records Management Systems**

Records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle; this includes any electronic records that are migrated across to new systems. Therefore, before procuring new systems or putting new processes in place, organisations should take into account the need to keep up with technological progress (e.g. new hardware, software updates) to ensure that records remain accessible and retrievable when required.

A records management system should ensure there are accurate audit trails of when records are created (i.e. the date that a document becomes a formal corporate record), accessed (e.g. a sign-out book, or automatic date modified note against file name for electronic records) and disposed of:

* records are grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. archiving or destruction.
* there are suitable storage areas so that records, whether physical or electronic, remain accessible and usable throughout their life cycle.
* access to records is controlled through a variety of security measures, for example, authorised access to storage and filing areas, lockable storage areas, user verification, password protection and access monitoring.
* issue from and return to storage areas on site or to authorised off-site facilities is documented.
* technological upgrades are supported so that records remain accessible and usable throughout their life cycle.
* cross-referencing of electronic records to their paper counterparts is permitted (where dual systems are maintained).

Another objective of the records audit is to ensure that the organisation has complete and accurate corporate records to:

* enable internal and external audit.
* protect the legal rights of the organisation, its employees, its patients and third parties.
* provide authentication so that actions may confidently be taken on reliable information.

Actions taken to deal with identified problems should feed into the organisation’s information lifecycle management strategy (see **requirement 105**).

The records audit may reveal information held by or on behalf of another organisation, which may assist when responding to Freedom of Information requests (see **requirement 603**).

**A Records Audit**

The best approach to an audit of corporate records and information may be to set it up as a work programme in its own right. However, first there must be a formal commitment from senior managers supporting the process and delegating responsibility for coordinating and carrying it out to an appropriate member of staff.

To ensure the audit works effectively and achieves its aims, organisations should consider using established project management methodology and as such a Project Initiation Document (PID) and project plan should be developed and signed off by senior management. The PID and project plan should outline the commitment to allocate the necessary resources, both financial and human, to carry out the work and will need to identify:

• the aims and objectives of the audit.

• how staff members in relevant areas will be informed of the audit.

• the staff members/job roles responsible for undertaking the audit.

• how the audit will be carried out, for example, visits, questionnaires, interviews.

• the order that departments will be surveyed, (e.g. are there particular corporate areas that need to be done first?)

• the timescales for completion.

• how the finished work will be presented.

• who the finished audit will be presented to.

Once the PID and project plan have been signed off by senior managers and staff members in relevant areas have been effectively informed, work should commence based on the PID and project plan.

**Performing the Audit**

There are several ways in which an organisation may want to carry out the audit. An initial walk-through visit to the department selected for audit will enable the organisation to:

• see where paper and electronic records are stored.

• assess the general condition of stored paper records.

• obtain an overview of the types of information captured in the record.

Questionnaires and/or interviews can be used to gather detailed data, for example:

• who “owns” the record?

• how old is the record, i.e. what are the covering dates?

• is it still in use?

• is it of historical interest?

A records audit survey template and forms are available within the **Knowledge Base Resources** to enable organisations to gather data.

To assess the effectiveness of the audit methodology, organisations may wish to audit one corporate area first as a pilot.

It might be necessary to carry out follow-up interviews once the records audit survey results have been returned to the team co-ordinating the work.

A representative sample of the categories of record created by the chosen area should be tracked through the various departments and personnel that handle it, with particular emphasis on the type of information, what it is used for and, if it is passed on, who it is transferred to. If the information is copied or stored by any of the departments this should also be recorded, as this will assist organisations to more easily locate duplicates.

By tackling the work in “chunks”, an organisation can incrementally begin to build up a picture of corporate records, the information it holds and the information it sends and receives.

A report should be presented to the Board, senior management team or delegated sub-group, so that a decision can be made about the allocation of resources necessary to continue the work. The rate at which the organisation can audit further information and records will obviously depend on the resources available.

|  |  |  |
| --- | --- | --- |
| **Knowledge Base Resources Key Guidance** | | |
| **Title** | **Details** | **Last Reviewed Date** |
| DH: Records Management NHS Code of Practice for health and social care | The Code is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type. | 10/08/2021 |
| DH: Records Management Code of Practice | The Code of Practice comprises of ‘how to’ materials in the form of templates and checklists to assist organisations in developing and implementing solid records management processes. | 19/09/2023 |

|  |  |  |
| --- | --- | --- |
| Lord Chancellor's Code of Practice on the Management of Records, Issued under Section 46 of the Freedom of Information Act 2000 (archived site) | The Code sets out the practices that organisations should follow in relation to the creation, keeping, management and destruction of their records. Section 10 deals with knowing what records are held. | 15/07/2021 |
| Secretary of State for Constitutional Affairs: Code of Practice on the Discharge of Public Authorities' Functions under Part I of the Freedom of Information Act 2000 | The Code covers such issues as public authorities' duties in providing advice and assistance to applicants, charging fees, timeliness in answering requests, and transferring requests to other public authorities. | 23/12/2014 |
| The National Archives: Records Management Standards | The National Archives produces standards and guidance on all aspects of records management. These represent best practice and focus on public. | |

**Freedom of Information**

Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000.

**Guidance - Compliance with the Freedom of Information Act 2000**

**Introduction**

The Freedom of Information Act 2000 (FOIA) came into force at the beginning of 2005 and deals with access to information held by public authorities, for example, the NHS, the police, local government, and schools.

As a means of providing access to information, the Act also requires public authorities to have an approved publication scheme which is a means of providing access to information which is proactively published as part of its normal business activities.

Organisations should also take note of the effect of section 102 of the Protection of Freedoms Act 2012, which added new provisions to the FOIA (particularly to sections 11 and 19), see **paragraph 19** below. The changes are all about datasets, a term defined in the legislation. The Information Commissioner’s Office (ICO) has published guidance on the changes, which is available in the **Knowledge Base Resources**.

**Responsibilities for Freedom of Information Act Compliance**

The Chief Executive (or equivalent) has the ultimate responsibility for their Public Authority’s compliance with the Act and should ensure that responsibility for reporting Freedom of Information issues to the Board (or equivalent) is delegated to an appropriate Director (or equivalent) to act as Freedom of Information lead.

**Freedom of Information Lead**

The senior management level lead should ensure organisational procedures and processes are in place to comply with the Act. The key responsibilities are to:

• ensure that the organisation complies with all aspects of the Act, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings etc.

• provide reports to the Board (or equivalent) highlighting resource, performance and compliance issues.

• draft and / or maintain the currency of the organisation's policy.

• ensure that all staff are aware of their personal responsibilities for compliance with the Act and adhere to organisational policies and procedures.

• ensure training and written procedures are widely disseminated and available to all staff.

• ensure the general public has access to information about their rights under the Act.

• establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times.

• liaise and work with other functions responsible for information handling activities, for example the Caldicott Guardian, data protection and information security staff.

• contribute to or liaise with external FOI networks or groups to keep updated on circular (round robin) requests (see **paragraph 37**).

**Freedom of Information Manager/Staff**

For large or complex organisations, for example NHS Trusts, an individual should be nominated to manage the FOI process and support staff, and routinely report to the FOI Lead and Board (or equivalent).

**All Directors and Heads of Service (and equivalents)**

All corporate information, for example contracts and commercially sensitive information should be created with the awareness that a request for this information may be received and information which is not exempt must be disclosed to comply with the Act. Senior members of staff should therefore ensure that they (and their staff) receive adequate training to ensure they are able to adhere to policies, procedures and guidance.

**All Staff Members**

All staff should be made aware of their own personal responsibilities for the creation of records including emails which may be subject to and disclosed in response to an FOI request. In addition, each member of staff should be aware of the organisation’s process for dealing with a request which is received by them, for example who to contact and the urgency for doing so due to the strict time limits which the law applies.

**Information Governance Committee / Group**

* 1. The Information Governance Committee/Group should receive regular FOI performance reports which highlight:
* numbers of FOI requests received.
* numbers responded to within the 20 working day limit and the reasons for any exceeding the statutory deadline.
* the justification for the application of any exemptions.
* details of any complaints made about any response or the process itself.
* details of any requests that have been escalated to the Information Commissioner's Office by the applicant.
  1. Based on these reports the IG Committee/Group should agree any necessary improvement plans recommendations for improvements, for example identify additional resources if there is continued failure to meet statutory deadlines, increasing staff awareness through additional training or guidance materials

**Staff Training and Awareness**

* 1. For most large public authorities, comprehensive training should be provided for staff working in areas where requests are managed. The training should cover:
* recognising and responding to a request for information.
* developing and maintaining a Publication Scheme.
* records management.
* exemptions – public interest and absolute exemptions.
* complaints / enforcement.
* the interface between freedom of information and data protection.
* vexatious/repeated requests.
* fees.
  1. FOI support staff who may assist with locating and collating information should receive basic training in FOI issues.

**Publication Schemes**

The FOIA requires every public authority to adopt and maintain a publication scheme, and to publish information in accordance with the scheme. All public authorities must use one of the model publication schemes created by the Information Commissioner’s Office (ICO).

The amendments to the FOIA from the Protection of Freedoms Act 2012 require public authorities to publish any requested datasets as part of their publication scheme, if appropriate. Further guidance is in the **Knowledge Base Resources**.

The model scheme is suitable for all sectors and consists of seven commitments and seven classes of information that must be published. The classes of information cover areas such as what services an organisation offers, how much it spends, its priorities, etc.

* 1. As well as making their publication scheme available to the public, (e.g. by placing a link to it on their website or otherwise making it available), organisations should also:

a. produce a **guide to information**, (or ensure that an existing website meets this need) that specifies the particular information the organisation publishes, how it will be published and how it is available, for example, online or by contacting the organisation by post; and

* + - 1. b. provide a schedule of fees, saying what the organisation charges for information.
      2. c. ensure that members of the public can easily obtain the information.
  1. To help organisations decide what should be included in a guide to information, the ICO has produced definition documents for various public sector bodies, such as central and local government, education, health, and the police. These set out the types of information the ICO would normally expect particular types of public authority to publish. A guide to using the definition documents is available in the **Knowledge Base Resources**.
  2. Organisations should maintain a log of requests, referred to as a disclosure log, with a view to making this publicly available. A publicly available disclosure log may help to reduce the numbers of similar requests (for example MRSA rates, bed numbers) an organisation receives as the information will be easily accessible and a separate request may therefore be unnecessary.

**The Protection of Freedoms Act 2012 amendments to FOIA**

Section 102 of the Protection of Freedoms Act 2012 amended sections 11 and 19 of the Freedom of Information Act, giving new rights to receive datasets in a form capable of re-use (e.g. in a CSV file). The Act gives users the right to re-use datasets, under the terms of a specified licence - in most cases likely to be the Open Government Licence (OGL). The amendments also require public authorities to publish any requested datasets as part of their publication scheme, if appropriate.

It is important to note that the changes do not give new rights of access - they are concerned with the format of, and the ability to re-use datasets, once the public authority has decided that no exemptions or other provisions (e.g. costs, vexatious request) in the legislation apply. See the **Knowledge Base Resources** for links to further detail and supporting information.

**Provision of Advice and Assistance**

The public may or may not be aware that information is available to them under the FOIA 2000. All organisations should assist in the communication of this fact by widely publicising the way in which the public may gain access to information covered by the Act. Organisations should have materials to support communications about FOI applications, supported by FOI request handling procedures.

Organisations also have an obligation to assist the public with making a request, for example if a request is made verbally by someone who is unable to read or write. In this case, an organisation should assist the applicant to write down their request and encourage him/her to verify with a friend or family member that the written request is in fact what is required. A similar approach can be taken with applicants who may not speak English and require assistance to write down their request.

It is particularly important that clinical / care staff members, and others dealing directly with patients and the public, are fully informed of the duty to provide advice and assistance.

Organisations should develop clear, publicly available, request handling procedures that are formally documented. The procedures should address the making of a FOI application and describe how such an application will be handled by the organisation. They should also address issues such as refusal of requests, the organisation's duty to provide a notice if a request is refused and provide a route for the applicant to make a complaint or lodge an appeal with the Information Commissioner.

**Recognising and Responding to Requests for Information**

The FOIA 2000 confers two rights on the general public: the right to be informed whether a public body holds certain information;

a. the right to obtain a copy of that information.

All organisations should aim to ensure that: the majority of information is made available through the organisation's guide to information;

a. other information is readily available on request;

b. if the information requested is assessed to be currently subject to an exemption, the organisation should provide a process to enable a judgement to be made as to whether the information can be released.

Where possible the information should be supplied in the format requested by the applicant. However, requests can be met by providing a copy of the original document, a digest/summary of the original or even by allowing the applicant to visit the organisation to read the document(s).

Requests for information should be met within 20 working days of receipt of the request or, where a fee is charged, within 20 working days of receipt of that fee. Additionally, if the organisation requires further clarification to enable it to identify the information requested, the 20 working days will not begin to run until the applicant has provided that clarification.

Responding to a request within the limits requires that the organisation can quickly locate and retrieve information. This Requirement is therefore dependent on work carried out to meet Corporate Information Assurance **requirement 604** related to the audit of information held by an organisation, and Corporate Information Assurance **requirement 601** regarding the effective management of corporate records. Where different personnel are in place, there will need to be appropriate links between the records management and the freedom of information functions to ensure that the most up to date information is available via the publication scheme and that any information that is updated, replaced or otherwise altered is made known to FOI staff so that it can be replaced in the publication scheme.

The person responsible for responding to FOI requests may also receive requests that should be handled under the Environmental Information Regulations 2004, e.g. information about clinical waste or incineration services. These requests can be made verbally and must be responded to within 20 working days of receipt. However, such requests may be dealt with elsewhere in the organisation, if so; FOI Leads should ensure they liaise with other staff members so that all requests for corporate information are dealt with consistently.

The Information Commissioner has published three documents to assist organisations in recognising and responding to FOI requests. The guidance documents are available in the **Knowledge Base Resources**. See 'Recognising a request made under the FOI Act'; 'Interpreting and clarifying requests'; and 'Means of communicating information'.

**Fees**

Organisations are permitted to charge reasonable fees to meet some of the cost of providing information and may charge for reasonably incurred costs to:

* inform the applicant whether the organisation holds the information.
* communicate the information to the applicant.
* the cost of putting the information into the applicant's requested format, e.g. CD, audio tape.
* photocopying and printing costs (set at no more than 10 pence per page).
* postage or other transmission costs.

The fee may include:   
  
Additionally, organisations may not charge for putting the information into another format if they are already under a duty to make information accessible under other legislation, e.g. the Disability Discrimination Act 1995. Furthermore, if organisations have an internal translation service, it would not be reasonable to charge a fee for translation into a language provided by members of that service.   
  
The Freedom of Information (Release of Datasets for Re-use) (Fees) Regulations 2013, (available in the **Knowledge Base Resources**), set out what a public authority can charge for making certain datasets available for re-use - the costs they can recover and a reasonable return on investment.

**Complex or Costly Requests**

There may be a few cases where the costs of meeting a request would exceed the appropriate limit, set at £450. If this is the case, organisations may be exempt from answering the request.

The limit is applied first to the organisation's duty to confirm or deny that it holds the information and then to its duty to supply the information. Therefore, if it would cost more than £450 to confirm or deny then there is no duty to do so.

Organisations are permitted to estimate whether the cost of meeting a particular request would exceed the £450 limit. To do this they should take into account the costs of employing staff to:

a) determining whether you hold the information;

b) finding the requested information, or records containing the information;

c) retrieving the information or records; and

d) extracting the requested information from records

To estimate these staff costs organisations should use an hourly rate of £25 per person per hour, that is, a limit of 18 staff hours. In making this estimation, no other costs may be taken into account.

**Exempted Information**

Organisations may receive requests for information that are judged to be exempt from release; however, the relevant information should be kept under review, as it may be possible to release it in the future. This may include information provided by third parties given with the expectation that it would be held in confidence, for example, tenders for contracts before the contract has been awarded. Once the contract has been awarded, it might be possible to release the successful and unsuccessful tenders if a request is made.

**Complaints and Appeals**

The Freedom of Information Act does not require an authority to have a review procedure in place. However both the Code of Practice made under section 45 of the FOIA 2000 and the Information Commissioner’s Office recommend it is good practice to have one. Section 17(7) of the FOIA provides that, in a refusal notice, an authority must give details of any review procedures, as well as details of the right of appeal to the Information Commissioner.

Organisations should assign responsibility for dealing with any complaints and appeals, e.g. initial complaints about the organisation's FOI procedures and appeals against decisions not to supply exempt information. If the lead is unable to resolve the issue the complaint/appeal should be referred to the organisation's IG committee (or equivalent) for consideration and involve the organisation’s Complaints Officer/Manager.

**Circular (Round Robin) Requests**

Staff that manage FOI requests should be alert to the possibility that a request may have been sent to a number of organisations i.e. circular or 'round robin’ requests. The Information Commissioner has issued guidance on ‘Circular requests’ and advises that if a request is valid, any consideration of whether it is vexatious or manifestly unreasonable should be carried out in accordance with their separate guidance on ‘Dealing with vexatious requests’ and ‘Manifestly unreasonable requests’. These three guidance documents are all available via the **Knowledge Base Resources**.

|  |  |  |
| --- | --- | --- |
| **Knowledge Base Resources Key Guidance** | | |
| **Title** | **Details** | **Last Reviewed Date** |
| Information Commissioner: Guide to the Freedom of Information Act | This guide is for those who work for a public authority and have day-to-day responsibility for freedom of information. It explains how to apply the Act by giving practical examples and | |

|  |  |  |
| --- | --- | --- |
|  | answering frequently asked questions. | |
| DH: Records Management NHS Code of Practice for health and social care | The Code is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type. | 10/08/2021 |
| DH: Records Management Code of Practice | The Code of Practice comprises of ‘how to’ materials in the form of templates and checklists to assist organisations in developing and implementing solid records management processes. | 19/09/2023 |
| Freedom of Information Act 2000 | An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes. | 25/09/2023 |
| Ministry of Justice: Freedom of Information Pages | Guidance and resources to help those who work in central government, or other public authorities, to deal with freedom of information requests. | 25/09/2023 |
| Information Commissioner: FOI - Model Publication | These set out the types of information the ICO would expect particular types of authority to publish and list | 23/10/2015 |

**Registration Authority**

There are established business processes and procedures that satisfy the organisation’s obligations as a Registration Authority

**Requirement Description**

This requirement addresses the obligations placed on an organisation that has Registration Authority (RA) responsibilities. RA responsibilities should be managed as an organisation Information Asset, by the

assigned Information Asset Owner (IAO), or equivalent and should be identified in the organisation’s Information Asset Register. The IAO will further ensure that individuals assigned RA responsibilities, have sufficient skills and access to knowledge to perform their roles, that there are procedures to ensure all NHS Smartcards and access profiles are issued appropriately and that RA equipment (hardware and software) and consumables meet current specifications, are adequately maintained, subject to business continuity and contingency planning needs, and are securely stored.

**Guidance - Obligations of a Registration Authority**

**Introduction**

A Registration Authority manages the registration and access control processes required to ensure that individuals who need to access computer systems linked to the NHS Spine have had their identity rigorously checked and are assigned appropriate access according to the user’s business need.

To satisfy its obligations as a provider of Registration Authority services, the organisation should establish local registration services are carried out in accordance with National Registration Authority Policy (see the **Knowledge Base Resources**), Data Protection Act 1998, Department of Health RA policy, the NHS Care Record Guarantee for England and the NHS Employment Check Standards.

To ensure there is adequate governance, the Registration Authority business processes and procedures should be embedded within the organisation's Information Governance Framework.

There are principles and rights set out in the NHS Care Record Guarantee and NHS Constitution that govern how patient information is used (in England) and the controls patients can have over this. These principles and rights apply to personal information held in all forms, including electronic records held on computer systems linked to the NHS Spine.

**NHS Care Record Guarantee for England**

Individuals’ rights regarding the sharing of their personal information are supported by the NHS Care Record Guarantee, which sets out high-level commitments for protecting and safeguarding patient information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

**Roles and Responsibilities**

There should be an IAO assigned overall responsibility for the organisation’s RA. This individual should also be a member of the Board to report to the organisation's Board on RA matters in person.

To ensure adequate governance, senior members of staff and appropriate areas of the organisation should also be involved, such as the Senior Information Risk Owner, the Caldicott Guardian, Human Resources Director, Clinical Directors and the IM&T Director.

The RA Manager and Sponsor roles need to be assigned to trusted individuals and formally recorded by the local Executive Management Team.

The responsibilities of an RA Manager are to assign, sponsor and register RA agents and assist Sponsors in understanding Role Based Access Control (RBAC) and Position Based Access Control (PBAC), by the development of access control positions, and in finding information about applications they sponsor Users for.

The RA Manager is also responsible in developing and updating the organisation’s RA policy and processes ensuring that is aligned to the National RA policy and processes.

As a minimum the local RA policy should address the following:

a. Executive Appointment of RA Manager and Sponsors.

b. RA staff and Sponsor responsibilities.

c. Audit policy including annual audits.

d. Training.

e. Safe haven arrangements to store documents and hardware.

f. Hardware and Software requirements.

g. Align to the organisation’s employment terms and conditions.

h. Staff compliance with NHS Smartcard Terms and Conditions of use and measures to ensure compliance.

Organisations receiving the RA service are made aware of their responsibilities to:

i. Monitor staff compliance with the terms and conditions of NHS Smartcard use.

ii. Inform the issuing organisation when staff leave or change jobs.

iii. Report any NHS Smartcard related security events/issues.

As a minimum the local RA procedure should consist of the following:

a. Registration of Users.

b. Starters and Leavers Processes.

c. Alignment to organisations leavers and joiners policy.

d. Secure methods to transfer NHS Smartcards to Users in accordance to the organisations secure methods of transfer policy or equivalent policy.

e. Incident Reporting.

f. The organisation’s Service Management process.

g. Password management including Self Service Portal.

h. Certificate Renewals including Self Service Portal.

Detailed information on the roles of the RA Manager, RA Agent and Sponsor can be found within the RA Process Guidance available in the **Knowledge Base Resources**.

**Registration Authority Staff Knowledge, Skills and Training**

Organisations must both identify, and provide for, the training needs of staff involved in the establishment and management of Registration Authorities. This will include ensuring staff have access to the latest software, national e-learning, the national RA Policy and the latest RA Process Guidance

(available via the **Knowledge Base Resources**), and the integration of these into the organisation’s RA policy and RA procedures.

The level of knowledge and skills required by staff involved in the set up and management of Registration Authorities will vary according to the role or position they occupy and their overall responsibilities, set out in the RA Policy and RA Process Guidance (available via the **Knowledge Base Resources**).

Guidance and training materials are provided by HSCIC. As noted earlier, it is the responsibility of the RA Manager to ensure that Agents and Sponsors are sufficiently trained e.g. by providing “train the trainer” courses or ensure that staff complete the available e-learning appropriate to their role.

**RA Business Processes: Registration of Users**

An organisation’s RA processes must be reliable and robust to ensure that sufficient, but not excessive, access is provided for staff to carry out their duties. Local RA processes must be consistently interpreted into high standards of practice, and, where access is amended or withdrawn, without delay.

RA Service Providers providing a RA service to other organisations should ensure that practice partners, owners, senior managers, etc are aware of and comply with their responsibility to monitor staff compliance with the RA/ NHS Smartcard terms and conditions; to inform the relevant RA Service Provider when staff leave or change jobs, and to report any NHS Smartcard related security events/issues (see **requirement 304, or 360 depending on organisation-type**).

Detailed guidance on the requirements necessary where the RA service is provided on behalf of another organisation are set out in the RA Process Guidance available in the **Knowledge Base Resources**.

**RA Business Processes: Care Identity Services (CIS)**

All organisations are required to assure the identity of individuals involved in the provision of NHS services, for which that organisation is responsible as per the latest version of the NHS Employment Check Standards in the **Knowledge Base Resources**.

Position Based Access Control (PBAC) must be defined by an organisation’s RA. PBAC provides a simple and effective mechanism for providing users with the access they need, whilst also ensuring that these access rights are properly managed and appropriate for the job they are doing.

PBAC is a pre-requisite to use the Care Identity Services (CIS) application. Information on implementing CIS is available in the RA Process Guidance and CIS User Guide in the **Knowledge Base Resources**.

**RA Business Processes: Availability of Equipment and Consumables**

To provide a reliable and robust RA Service, the RA Manager should ensure that there is a sufficient supply of NHS Smartcards, RA hardware and consumables to support the activities of all authorised NHS Smartcards. The RA Manager should communicate technical requirements to the Information

Technology Team. The IT Manager will need to ensure that there is sufficient computer equipment and appropriate software to support RA registration services.

Should the RA responsibilities extend to provision of a RA service to Independent Contractors and Business Partners including general practices, community pharmacies and independent sector health service providers, then a written contract or service level agreement must be developed as this will influence the levels of NHS Smartcards and Smartcard readers stock availability needed. .

**RA Business Processes: Security of Equipment and Consumables**

Organisations must ensure that equipment such as computers, Smartcard readers and NHS Smartcards are protected (see also **requirement 323**). To ensure access to national applications is managed securely, it is imperative that NHS Smartcard processing forms and documentation are controlled.

Any incident relating to the loss or theft of RA equipment (including issued and non-issued NHS Smartcards) or documentation should be reported and the RA Manager informed immediately so that appropriate security measures (e.g. NHS Smartcard cancellation) can be taken.

All personal and sensitive non-personal information (e.g. historical completed User Registration Forms, lists of RA staff including sponsor, inter-organisation agreements), received or recorded for RA purposes must be adequately protected in accordance with the organisation’s information security or equivalent policy.

Historical RA forms must be clearly marked with the user’s UUID number and checked for completeness before filing. They must be handled and stored securely at all times with access restricted to RA and/or HR staff. They can, if it is undertaken to the relevant British Standard, be scanned and stored electronically and the physical copies then destroyed. Retention periods are shown in the Records Management: NHS Code of Practice, available via the **Knowledge Base Resources**.

* 1. All RA equipment must be adequately protected in accordance with the organisation’s information security or equivalent policy e.g.:

1. Mobile RA equipment must be adequately protected at all times and not left unattended on sites or in the boot of a car.
2. NHS Smartcards should be removed from the printer.
3. Any paper RA forms should always be kept separate from the registration equipment when transporting from site to site to avoid security issues.
4. NHS Smartcards should be kept in a secure locked unit when not required.

All RA equipment including NHS Smartcards to be securely distributed in accordance with the organisation’s secure method of transfer or equivalent policy.

|  |  |  |
| --- | --- | --- |
| **Knowledge Base Resources Key Guidance** | | |
| **Title** | **Details** | **Last Reviewed Date** |
| DH: Information Security NHS Code of Practice 2007 | The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual. | 21/11/2018 |
| NHS Employment Check Standards | The NHS Employment Check Standards outline the employment checks employers must carry out before appointing staff into NHS positions, across England. This includes NHS positions for permanent staff, staff on fixed-term, volunteers, students, trainees, contractors, highly mobile staff, temporary workers (including locum doctors), those working on a trust bank, and other workers supplied by an agency. | 26/04/2023 |
| NHS Employers: Identity Check Standards | This document outlines the identity checks that NHS organisations (across England) are required to undertake in the appointment and ongoing employment of individuals in the NHS. It is one of a set of six documents that make up the NHS | 26/04/2023 |

**Smart Card Guidance**

Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.

**Requirement Description**

All organisations need to ensure that staff members and those working on behalf of the organisation issued with an NHS Smartcard comply with the terms and conditions of issue. Breach of the terms and conditions and/or of organisational procedures relating to NHS Smartcard usage should be linked to disciplinary measures.

**Guidance - NHS Smartcards**

**Introduction**

NHS Smartcards and passcodes help control who can access the NHS Care Records Service (CRS) applications and what level of access that they can have. Before an NHS Smartcard is issued, the Registration Authority (RA) requires applicants to accept Care Identity Services (CIS) terms and conditions of issue.

**Compliance with the Terms and Conditions of NHS Smartcard Issue**

These conditions are in part no more than the information governance practice required of all staff but there are also a number of key requirements around the safe and secure retention of NHS Smartcards and the notification of any changes to the user’s access profiles.

It is essential that everyone with an NHS Smartcard and passcode is aware of and able to comply with the terms and conditions of issue and that they understand that failure to do so will be dealt with as a serious disciplinary matter.

If the NHS Smartcards and passcodes have been issued via another organisation’s RA (e.g. by a RA Service Provider organisation to a general practice, dental practice, eyecare service, community pharmacy, independent sector care provider, or voluntary sector organisation), then the issuing organisation will require assurances. These assurances will include evidence of periodic review that practice partners, owners, senior managers, etc. are aware of and complying with their responsibilities as set out in the issuing organisation’s RA policy to:

a. Monitor staff compliance with the terms and conditions of NHS Smartcard usage.

b. Inform the issuing organisation when staff leave or change jobs.

c. Report any usage issues.

All organisations, that have NHS Smartcard users must have effective and clearly defined procedures for monitoring staff compliance with the terms and conditions of NHS Smartcard usage and dealing with breaches such as the misuse of NHS Smartcards and passcodes. These procedures need to be organisation-based so that appropriate action can be taken by the user’s employer and should integrate with existing Human Resources and information security procedures.

All NHS Smartcard users must be effectively informed about the procedures for dealing with a breach.

**Community pharmacies**

Community pharmacies should note that in Release 2 of the Electronic Prescription Service (EPS), dispensing contractors will have access to a part of the NHS CRS known as the Personal Demographics Service. To obtain access rights to EPS Release 2 functionality, dispensing contractors and their staff will be required to adopt the ‘single Smartcard’ access model and sign up to the conditions set out electronically.

**Determining Whether the Requirement Can be Marked 'Not Relevant**

This requirement can be marked “Not Relevant” (NR) if NHS smartcards are not used by the organisation.

**Please note:** it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

|  |  |  |
| --- | --- | --- |
| **Knowledge Base Resources Key Guidance** | | |
| **Title** | **Details** | **Last Reviewed Date** |
| Registration Authority policy  (http://nww.hscic.gov.uk/rasmartcards/docs/rapolicyv1sep14.pdf) | (NHS Network users only): This document lays out the RA Policy requirements which every organisation that has a Registration Authority needs to adhere to. | 04/07/2023 |
| Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013 (PDF, 373 KB) | BSI UK document showing the mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013 | 25/10/2022 |
| Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 (PDF, 497 KB) | BSI UK document designed to help meet the requirements of the new international standard for information security management, ISO/IEC 27001:2013, which is the first revision of ISO/IEC 27001:2005. | 25/10/2022 |

# APPENDIX 1

**Data Protection Act 1998 – Principles**

A summary of the eight principles of the Data Protection Act 1998 is given below. To see these principles in their entirety, please follow the link below:

<http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_9#sch1-pt1>

Data:

1. Processed fairly and lawfully

2. Processed of specified purposes

3. Adequate, relevant and not excessive

4. Accurate and kept up to date

5. Not kept for longer than necessary

6. Processed in accordance with the rights of data subjects

7. Protected by appropriate security (practical and organisational)

8. Not transferred outside the EEA without adequate protection