Data Security Standard 1

Personal confidential data

The bigger picture and how the standard fits in

2018
## Contents

### Overview

#### Leadership

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tone from the top of your organisation</td>
<td>4</td>
</tr>
<tr>
<td>Senior Information Risk Owner role</td>
<td>5</td>
</tr>
<tr>
<td>Caldicott Guardian role</td>
<td>6</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>7</td>
</tr>
<tr>
<td>Do we need to have a Data Protection Officer?</td>
<td>7</td>
</tr>
<tr>
<td>If you choose not to Appoint a Data Protection Officer</td>
<td>8</td>
</tr>
<tr>
<td>What about IG Leads?</td>
<td>9</td>
</tr>
</tbody>
</table>

### Policies

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual rights and the Regulator</td>
<td>11</td>
</tr>
<tr>
<td>Regulator - the Information Commissioner</td>
<td>12</td>
</tr>
<tr>
<td>Individual rights</td>
<td>13</td>
</tr>
<tr>
<td>Transparency</td>
<td>13</td>
</tr>
<tr>
<td>Informing Individuals</td>
<td>14</td>
</tr>
<tr>
<td>Subject access</td>
<td>15</td>
</tr>
<tr>
<td>Data flow mapping</td>
<td>16</td>
</tr>
<tr>
<td>Information assets / systems</td>
<td>17</td>
</tr>
</tbody>
</table>

### Systems with no individual logins

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection guidance and monitoring</td>
<td>19</td>
</tr>
<tr>
<td>Organisations with Summary Care Record access</td>
<td>20</td>
</tr>
</tbody>
</table>

### Data protection and security by design

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical and physical access controls</td>
<td>23</td>
</tr>
<tr>
<td>Auditing pseudonymisation, anonymisation or de-identification controls.</td>
<td>25</td>
</tr>
<tr>
<td>Data protection impact assessments</td>
<td>26</td>
</tr>
</tbody>
</table>

### Data quality

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>29</td>
</tr>
<tr>
<td>Records Management</td>
<td>30</td>
</tr>
<tr>
<td>The records / information lifecycle</td>
<td>30</td>
</tr>
</tbody>
</table>

### Appendix 1 - Table of Data Security Level 5 Assertions

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1 -</td>
<td>34</td>
</tr>
<tr>
<td>Table of Data Security Level 5 Assertions</td>
<td>34</td>
</tr>
</tbody>
</table>

### Appendix 2 - Useful resources

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 2 -</td>
<td>39</td>
</tr>
<tr>
<td>Useful resources</td>
<td>39</td>
</tr>
</tbody>
</table>

### Appendix 3 - The National Data Guardian reports

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 3 –</td>
<td>41</td>
</tr>
<tr>
<td>The National Data Guardian reports</td>
<td>41</td>
</tr>
</tbody>
</table>
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.

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

Tone from the top of your organisation

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

The individual roles at a senior level that are relevant are those of the Senior Information Risk Owner (SIRO) and Caldicott Guardian.

Neither role is new in Health, but they are not widely known in Social Care.

Dependent on the size of your organisation you may need to combine these roles, potentially with the Information Governance Lead.

The person who takes on these roles does not have to be the Registered Manager, but should either report to, or be a part of, the senior management team so that they can complete their tasks.

There is more detail on these roles below.

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

NDG Review
Senior Information Risk Owner role

The Senior Information Risk Owner (SIRO) should be a senior member of the board or part of senior management team.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks.

The SIRO will act as an advocate for information risk at the highest level.

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed. He/she will provide leadership and guidance.

The key responsibilities of the SIRO are to:

- oversee the development of data protection and associated policies – particularly focussing on information risk.
- take ownership of the risk assessment process for information and cyber security.
- review and agree action in respect of identified information risks.
- ensure that the organisation’s approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff.
- provide a focal point for the resolution and / or discussion of information risk issues.
- ensure that senior management is adequately briefed on information risk issues.
- ensure that all care systems’ information assets (a body of information which has value to an organisation, for example care records in a filing cabinet or on planning software) have an assigned Information Asset Owner- someone who is responsible for keeping them secure day to day. For example, care plans might be the responsibility of a unit manager or registered manager, employee records might be the responsibility of the administrator.
Caldicott Guardian role

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

All NHS organisations and local authorities providing social services must have a Caldicott Guardian who is required to be registered on the publicly available National Register of Caldicott Guardians. Other health and social organisations (e.g. from the independent sector) are encouraged to register a Caldicott Guardian but this is not mandatory.

There should be someone within your organisation who is responsible for ensuring that people's data rights are protected – this might be in a combined role with the SIRO or IG Lead etc.

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

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

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

There is more information on this in the Information Governance Alliance (IGA) guidance on DPOs.

Do we need to have a Data Protection Officer?

Under the GDPR, you must appoint a DPO if you:

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

If you are a Local Authority or NHS owned care provider, you will be required to appoint or have access to a DPO as you are classed as a public body. It is likely that your Local Authority or CCG will already have somebody in this role and you should discuss with them about access to these services.

Large social care providers are likely to need to appoint a DPO as part of their journey towards compliance. There is guidance on this role below.

For smaller care providers you should appoint somebody in a champion role – this might be your IG Lead or similar. Do not refer to this person as a DPO as this role has specific legal requirements. The person in this role will be responsible for championing compliance with data protection legislation within your organisation. It is important that they also understand the limits of their knowledge and know where they can go for more advice if required.

If you consider yourself to be a smaller organisation, you will need to record your reasoning for not appointing or having access to a DPO.

---

1 Public authorities are defined in the Freedom of Information Act 2000 and more information can be found here: https://ico.org.uk/media/for-organisations/documents/1152/publicAuthorities_under_the_foa.pdf
2 Note that there has not yet been a definition of what is meant by “large scale” and so there is some uncertainty around which size of provider would be expected to have a DPO.
The role and characteristics of a DPO

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

The DPO’s responsibilities include:

1) Informing and advising organisations about complying with GDPR and other data protection laws;
2) Monitoring compliance with GDPR and data protection laws – including staff training and internal audits;
3) Advising on and monitoring data protection impact assessments;
4) Cooperating with the ICO;
5) Being the first contact point for the ICO and citizens in terms of data processing.

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

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

There is more information about requirements for DPOs here:

Information Governance Alliance: [https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance](https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance)


If you choose not to Appoint a Data Protection Officer

You need to record your decision not to appoint a Data Protection Officer and why you came to that decision.

You should appoint a champion for data protection (similar to an IG Lead). Skills for Care have created a guidance document for the data protection champion role.

Name of Appointed Data Protection Officer.

Data Security Standard 1.1.6

---

3 GDPR Articles 37-40
What about IG Leads?

Information Governance Leads in smaller organisations will probably merge with the Caldicott Guardian and SIRO roles. There is still an expectation that the following duties will be carried out (irrespective of the name of the role).

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

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

   We appreciate that for small organisations it might be difficult for an individual to take this on as a large role. Small organisations should aim to have someone championing data protection and people’s data rights, they do not have to be an expert as long as they know where they can go for more information. Skills for Care are working to provide core competencies for what this role might look like.

3. Under the approved arrangements, the IG Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks of an IG Lead include:
   a. developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high-level strategy document supported by corporate and/or directorate policies and procedures;
   b. ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
   c. providing direction in formulating, establishing and promoting IG policies;
   d. establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives (more likely in larger organisations);
   e. ensuring annual assessments using the Data Security and Protection Toolkit and audits of DSPT policies and arrangements are carried out, documented and reported to commissioners if a contractual requirement;
   f. ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the board or senior management team in a timely manner;
   g. ensuring that the approach to information handling is communicated to all staff and made available to the public;
   h. ensuring that information governance staff understand the need to support the safe sharing of personal confidential data for direct care as well as the need to protect individuals’ confidentiality;
i. ensuring that appropriate training is made available to all staff and completed as necessary to support their duties. It is recommended that this training takes place annually. There is more guidance on staff training in the Picture Guide for Data Security Standard 3;

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

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

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

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

There is no set number of how many different policies you have on these topics, but it is important the policies are effective, acknowledged and understood.

It is also important they:

- are reviewed at regular intervals
- that your “live” policies are finalised (i.e. not draft)
- version controlled
- have not gone past their review date
- follow your approved process for policy ratification (like all your other policies) including SIRO endorsement
- where appropriate are linked to other corporate policies
- are available to staff.

In terms of transparency, ideally you would make your policies available to the public, you should decide if this makes sense for your organisation – remembering that it is at a minimum a legal requirement to provide people with information on how you use their data. Be careful of publishing any information on your cyber security online if this could cause a security breach.

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

- data protection including confidentiality
- freedom of Information (if the organisation is subject to the Act)
- data security
- records management
- acceptable use.
Individual rights and the Regulator

Regulator - the Information Commissioner

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

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

All social care providers are required to register with the ICO as data controllers.

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

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

There are clear data security and protection policies in place and these are understood by staff and available to the public.
Two things that GDPR embeds is respecting individual rights and the transparency of what happens to their personal data.

**Individual rights**

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

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

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

![Image](https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance)

**Transparency**

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

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


![Image](https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance)
Informing Individuals

This can be directly via correspondence or indirectly leaflets and websites.

Would include a list of rights and when/whether they apply to the processing undertaken by the organisation, contact details and procedure for subject access, and other rights requests.

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

Data Security Standard 1.3.3

There is a staff procedure about how to provide information about processing and individuals’ rights at the correct time.

Data Security Standard 1.3.4

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

Under GDPR, it is no longer possible to charge a fee for most Subject Access Requests and the time period to comply with a request is shortened to one month from 40 days.

Please see IGA GDPR checklist (10. Manage subject access requests).

There is an updated subject access process to meet shorter GDPR timescales.

Data Security Standard 1.3.5

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

Provide details of how access to information requests have been complied with during the last twelve months.

Data Security Standard 1.3.6

<table>
<thead>
<tr>
<th>For period dd/mm/yy to dd/mm/yy</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of SARs</td>
</tr>
<tr>
<td>No of SARs late</td>
</tr>
<tr>
<td>No of FOI</td>
</tr>
<tr>
<td>No of FOI late</td>
</tr>
</tbody>
</table>
Data flow mapping

There must be a record (e.g. register or registers) that details each use or sharing of personal information, including the legal basis for the processing and if applicable, whether the National Data Opt Out has been applied to any sharing of the data for secondary purposes (note that the National Data Opt-Out is not being applied to Adult Social Care until 2020 – more advice will be available before that date).

The record should include for each entry:

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

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

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

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

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

- The public will be able to set national data opt-outs from 25th May 2018.
- NHS Digital will be the first organisation to implement the national data opt-out on 25th May 2018.
- Other health and social care organisations will be required to implement by 2020. An implementation plan will be published on the national data opt-out website.
- Health and social care providers need to be prepared to handle enquiries from patients/service users once the national data opt-out is launched. Information and resources are available to organisations on the NHS Digital website. https://digital.nhs.uk/national-data-opt-out

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

Definitions and scope

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

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

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

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

Confidential personal information can be held in systems such as:

- Care administration systems
- staff rostering systems
- payroll

You should keep a record of all of the different types of personal confidential information you hold. This does not need to be on the level of an individual file, but in groups. For example, care records are stored in this filing cabinet, employee pay records are stored in this computer system.
There is not a prescribed method, however, this is usually done in an information asset register. It should include the following information:

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.

There is a template available for social care on the Care Provider Alliance website.

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

Data Security Standard 1.4.4
**Systems with no individual logins**

Systems that do not support individual logins by their very nature carry more risks than those that do.

These systems pose risks because generally:

1) they make audit and accountability difficult as you cannot guarantee who is making actions on the account

2) password management is troublesome, where effectively you cannot change a password without affecting other users (or a password is changed and affects other users). Invariably account sharing leads to more password sharing, with a potential for password disclosure outside the original group.

These systems should be known and stored on a list (again this can be an existing information asset register).

Each of the systems should include a risk assessment or description of each system which does not support individual logins. The control measures or mitigations should also be stated for each risk, have a risk assessment or description of the risk with its likely impact and likelihood. This should consider the type of system, the volume of confidential personal data and how and where this is accessed. The control measures or mitigations should also be stated for each risk.

An example risk assessment.

---

List of systems which do not support individual login with the risks outlined and what compensating measures are in place.

Data Security Standard 1.4.5
Data protection guidance and monitoring

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

This can range from general awareness campaigns:


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


You should also undertake spot checks and audits to see whether the guidance is being adhered to.

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

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

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

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

**Organisations with Summary Care Record access**

Every organisation that has access to Summary Care Records (SCRs) must have a nominated Privacy Officer Function that is responsible for monitoring the SCR viewing activity of their users. Individuals with the Privacy Officer role will be given access rights on their Smartcard to perform the activities necessary to manage alerts and audit SCR viewing activity. Alerts are generated by end users when they override one of the information governance controls that are in place. Therefore, activities that will trigger an alert include:

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

GDPR requires that all organisations implement data protection by design and by default. This means that systems should be designed to take account of data protection and security issues at the point of conception. Trying to retrofit controls to systems that have little consideration at the onset can be expensive, labour intensive and less seamless to the users of the systems.

Your data protection by design procedures should aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent, where feasible allowing individuals to monitor what is being done with their data. Together the procedures should enable your organisation to improve data protection and security.

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

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

Please see IGA GDPR checklist (3. Data protection by design and default and DPIAs). This procedure should be approved through your local governance process.

Data protection by design procedure agreed by local governance process.

Data Security Standard 1.6.2
Technical and physical access controls

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

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

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

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

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

Smartcard enabled access
Using smartcard and other forms (token etc.) of physical devices to introduce another factor in accessing systems. This is not commonly used across social care.

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

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

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

Using test data (where appropriate)
Using data that is completely unrelated to live data, such as for training.

Data loss prevention
A system that inspects data going outside the organisation and can report and/or block it.
Control of personal web-based email systems

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

Effective audit logging

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

Physical controls.

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

These can include (but is not limited to).

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

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

Data Security Standard 1.6.3

There are physical controls that prevent unauthorised access to sites.

Data Security Standard 1.6.4
Auditing pseudonymisation, anonymisation or de-identification controls.

An audit has occurred within the reporting year to review the implementation of pseudonymisation and anonymisation controls and ensure they are working effectively.

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

Overall findings of last audit of [pseudonymisation, anonymisation or de-identification] controls.

Data Security Standard 1.6.6
Data protection impact assessments

Data Protection Impact Assessments (DPIAs) are what were previously called Privacy Impact Assessments. They have not traditionally been commonly used in adult social care, but GDPR has introduced a duty to complete one when there is “high risk” processing.

“High risk processing’ encompasses:

• automated processing
• large scale processing of special categories data - which includes health and genetic data
• systematic monitoring of a public area.

As with Data Protection Officers above, it is not clear what it meant by “large scale” processing. For many small social care providers, it is unlikely that they will be considered to be doing large scale processing.

Nonetheless, it would be good practice to complete a DPIA when you are bringing in any new system which could impact on individual’s data rights, if you choose not to do so you should keep a record of why you made this decision.

If there is an existing process, it should be reviewed setting out under what circumstances to carry out a DPIA noting the GDPR requires:

• seek the advice of the DPO (if applicable) when carrying out an assessment
• consulting with the ICO where a DPIA indicates a high risk to individual rights and freedoms that cannot be mitigated.
The process should be compatible with ICO guidelines (such as the process above).

There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.

The Data Protection Impact Assessment Procedure has been agreed by the Board or equivalent.

The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessment is being carried out.

Have any unmitigated risks been identified through the Data Protection Impact Assessment process?

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

The process should be agreed at board or equivalent level.

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

It also important that the DPIA forms part of your data protection by design and any possible high-risk processing assessment occurs before processing commences.
If your DPIA identifies a high risk and you cannot mitigate that risk, you must consult the ICO before starting the processing. The ICO has stated that written advice will be provided within eight weeks, or 14 weeks in complex cases. In appropriate cases, the ICO may issue a formal warning not to process the data or may ban the processing altogether.

All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.

Data Security Standard 1.6.12

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

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

Data Security Standard 1.6.13

All high-risk data processing has a Data Protection Impact Assessment carried out before processing commences.

Data Security Standard 1.6.11
Data quality

Overview
CQC's Regulation 17: Good Governance is one of the fundamental regulatory standards in Adult Social Care.
As part of this standard, social care providers are required to keep accurate, contemporaneous records of care and that this is audited to maintain quality.

Guidance
Guidance on how to ensure you are meeting this standard is available on the CQC website: https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-17-good-governance#guidance

The scope of the data quality audit was in line with guidelines.

Overall findings of last audit of data quality.
Records Management

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

Function:

- health and care records (electronic or paper based, including those concerning all specialties and GP records)
- administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling)
- integrated health and social care records
- data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.
- a patient or staff genomic data or IP address.

Format:

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

The records / information lifecycle

Your records management framework should manage the records lifecycle, or the information lifecycle, which is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest (for those subject to the Public Records Act or FoI).
Arguably the biggest concern (from a data security and protection viewpoint) is towards the end of the lifecycle. There are plenty of high profile cases where records have been inappropriately disposed of, leading to a data breach or alternatively disposed of earlier than they should have been.

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

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


Your data disposal contracts and suppliers should reference or include guidance on disposal of electronic media containing personal or sensitive data.
Traditionally, paper-based disposal has consisted of simple vertical shredding. However, this method is not suitable for sensitive or confidential information.

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

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

The contracts themselves should be reviewed periodically as the devices that are disposed of will change as they reach the disposal stage.

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

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

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

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

Data Security Standard 1.8.3
Each disposed of item should be recorded on a destruction certificate.

It important to note this data destruction can be physical (such as shredding) but can also be wiping (to the recommended standard). Each destroyed asset should be recorded on a destruction certificate.

This can be one certificate per item but also can be multiple items on one certification. It is important these items are known and can be referenced individually.

So, destruction certificate with:

Not acceptable

- 50 x SATA mixed sized hard drive destroyed - there is no traceability.

Whereas line item will 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 -
### Table of Data Security Level 5 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Applicable</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 There is senior ownership of data security and protection within the organisation.</td>
<td>Yes</td>
<td>1.1.1</td>
<td>Name of Senior Information Risk Owner.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.1.2</td>
<td>SIRO Responsibility for data security has been assigned.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.1.3</td>
<td>Name of Caldicott Guardian.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.1.4</td>
<td>Who are your staff with responsibility for data protection and/or security?</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>1.1.5</td>
<td>Staff awareness - Leadership (Q1) I feel data security and protection are important for my organisation.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.1.6</td>
<td>Name of Appointed Data Protection Officer.</td>
</tr>
<tr>
<td>1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.</td>
<td>Yes</td>
<td>1.2.1</td>
<td>There is a data security and protection policy or policies that follow relevant guidance.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.2.2</td>
<td>When were the data security and protection policy or policies last updated?</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>1.2.3</td>
<td>Policies have been approved by the person with overall responsibility for data security.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>1.2.4</td>
<td>Data Security and Protection Policies available to the public.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>1.2.5</td>
<td>Staff awareness - Policies (Q2). I know the rules about who I share data with and how.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>1.2.6</td>
<td>Staff awareness – Policies (Q3). I know who to ask questions about data security in my organisation.</td>
</tr>
<tr>
<td>1.3 Individuals’ rights are respected and supported (GDPR Article 12-22)</td>
<td>Yes</td>
<td>1.3.1</td>
<td>ICO Registration Number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.3.2</td>
<td>Transparency information is published and available to the public.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.3.3</td>
<td>How have individuals been informed about their rights and how to exercise them?</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.3.4</td>
<td>There is a staff procedure about how to provide information about processing and individuals’ rights at the correct time.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.3.5</td>
<td>There is an updated subject access process to meet shorter GDPR timescales.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.3.6</td>
<td>Provide details of how access to information requests have been complied with during the last twelve months.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.3.7</td>
<td>Total ICO fines in last 12 months</td>
<td></td>
</tr>
</tbody>
</table>

### 1.4 Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>1.4.1</td>
<td>A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied.</td>
</tr>
<tr>
<td>Yes</td>
<td>1.4.2</td>
<td>Have information flows been approved by the SIRO or equivalent local method?</td>
</tr>
<tr>
<td>Yes</td>
<td>1.4.3</td>
<td>Date of when information flows were approved by the Board or equivalent.</td>
</tr>
<tr>
<td>Yes</td>
<td>1.4.4</td>
<td>Provide a list of all systems/information assets holding or sharing personal information.</td>
</tr>
<tr>
<td>Yes</td>
<td>1.4.5</td>
<td>List of systems which do not support individual login with the risks outlined and what compensating measures are in place.</td>
</tr>
<tr>
<td>1.5 Personal information is used and shared lawfully.</td>
<td>Yes</td>
<td>1.5.1</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Yes</td>
<td>1.5.2</td>
<td>Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed.</td>
</tr>
<tr>
<td>Yes</td>
<td>1.5.3</td>
<td>Results of staff spot checks and actions taken when data protection non-compliance is identified.</td>
</tr>
<tr>
<td>No</td>
<td>1.5.4</td>
<td>Staff awareness - Used legally and securely (Q4) .... I am happy data is used legally and securely in my organisation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.6 The use of personal information is subject to data protection by design and by default</th>
<th>Yes</th>
<th>1.6.1</th>
<th>There is a procedure that sets out the organisation’s approach to data protection by design and by default, which includes pseudonymisation requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>1.6.2</td>
<td>Data Protection by design procedure agreed by local governance process.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.6.3</td>
<td>There are technical controls that prevent information from being inappropriately copied or downloaded.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.6.4</td>
<td>There are physical controls that prevent unauthorised access to sites.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.5</td>
<td>Date of last audit of pseudonymisation, anonymisation or de-identification controls.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.6</td>
<td>Overall findings of last audit of [pseudonymisation, anonymisation or de-identification] controls.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.6.7</td>
<td>There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.8</td>
<td>The Data Protection Impact Assessment Procedure has been agreed by the Board or equivalent.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.9</td>
<td>The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessment is being</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>carried out.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.10</td>
<td>Have any unmitigated risks been identified through the Data Protection Impact Assessment process?</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.6.11</td>
<td>All high-risk data processing has a Data Protection Impact Assessment carried out before processing commences.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.6.12</td>
<td>All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.6.13</td>
<td>Data Protection Impact Assessments are published and available as part of the organisation’s transparency materials.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.7.1</td>
<td>There is policy and staff guidance on data quality.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.7.2</td>
<td>The scope of the data quality audit was in line with guidelines.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.7.3</td>
<td>Date of last data quality audit.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>1.7.4</td>
<td>Overall findings of last audit of data quality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.8.1</td>
<td>There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.8.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>-----------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td>A records retention schedule has been produced.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.8.3</td>
<td>Provide details of when personal data disposal contracts were last reviewed/updated.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

GDPR Checklist: Information Governance Alliance

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

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

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

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


GDPR checklist: Information Commissioner’s Office

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


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

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

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

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

Guidance covers:

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


Care Provider Alliance templates for social care providers

Guidance and templates. Includes template:

- Data Protection Policy
- Data Security Policy
- Data Quality Policy
- Record Keeping Policy
- Information Asset Register
- Record of Processing Activities

Appendix 3 –
The National Data Guardian reports

The NDG report

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

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.