The Care Provider Alliance
Working together for excellence and sustainability in social care

NHS Digital

Data Security and Protection Toolkit

Key roles and the DPO

2018

Information and technology
for better health and care

Contents

Key roles

The following key roles are included in the organisation profile of the Data Security and Protection Toolkit (DSPT). Below are details of the roles, their duties and which sectors or types of organisation are required to have one.

These roles are IG Leads, Caldicott Guardians, SIRO and Data Protection Officer.

Traditionally, the role of co-ordinating toolkit returns has fallen to the IG Lead. With the implementation of GDPR introducing the role of Data Protection Officer, it is expected that these roles will merge in larger organisations.

Information Governance Lead

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 response to the Caldicott 2 Review 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.

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

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

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

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

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

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

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

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

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

i. ensuring that appropriate training is made available to all staff and completed as necessary to support their duties. For NHS organisations, this will need to be in line with the mandate for all staff to be trained annually and should take into account the findings of The National Data Guardian review: "Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used", and the government's response to the review. Both documents can be downloaded from the big picture guides in the help section;

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

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

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

There is some overlap in this role with the new role of Data Protection Officer, and it will often be the same person in an organisation.

Information Governance Lead – social care providers

The Information Governance (IG) Lead can also be called the Data Security and Protection Lead or any equivalent title. The role can be similar to the “champion” role, which is seen in other areas across the sector. Each organisation’s IG Lead will be responsible for ensuring completion of the DSP Toolkit and has the responsibilities noted above.

In small organisations, the individual might also take on the responsibilities of the Caldicott Guardian function and the Senior Information Risk Owner (SIRO) role which are listed below.

The IG Lead 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.

Caldicott Guardians and the Caldicott function

1. The recommendations of the Caldicott Committee (1997 Caldicott Report) defined the confidentiality agenda for NHS organisations. A key recommendation was the appointment in each NHS Trust and special health authority (e.g. NHS Business Services Authority) of a “Guardian” of patient identifiable information to oversee the arrangements for the use and sharing of patient information. Guardians were mandated for the NHS in Health Service Circular 1999/012 and were introduced into social care in 2002, mandated by Local Authority Circular (LAC 2002/2).

2. In all other organisations, there should be access to expertise on Caldicott / confidentiality issues when required. This expertise might be provided by a member of staff acting as Caldicott Guardian, or by a Defence Union, or a legal advisor, etc. All organisations providing direct care to NHS patients are strongly encouraged to appoint a Caldicott Guardian, but if there is no in-house Guardian, there should be a confidentiality lead or ‘Caldicott function’ within the organisation to take overall responsibility for confidentiality issues and to seek additional advice when required. Senior members of a non-NHS organisation will be best placed to decide whether the role of Caldicott Guardian is assigned and / or whether external advice is sought if necessary. Paragraphs 11 - 15 below set out the member of staff that should ideally be assigned the role of Caldicott Guardian.

3. The Guardian should be, in order of priority:
    - an existing member of the senior management team;
    - a senior health or social care professional;
    - the person with responsibility for promoting clinical governance or equivalent functions.

4. The Guardian plays a key role in ensuring that the NHS, Councils with Social Services and Public Health Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

5. The Caldicott Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly important in relation to the implementation of national systems.

6. The Caldicott Guardian also needs to take into account the findings and recommendations from Dame Fiona Caldicott’s second review of information

governance in 2013 (the Caldicott 2 review). Importantly, the review introduced a new Caldicott principle to be used alongside the other six principles when testing whether identifiable information should be used or disclosed. The new principle states that the duty to share information can be as important as the duty to protect patient confidentiality. This means that where there is a duty to share, organisations should do so, rather than failing to share due to perceived confidentiality issues.

7. In all but the smallest organisations, the Caldicott Guardian should work as part of a broader Caldicott function with support staff, Caldicott or Information Governance Leads etc., contributing to the work as required. The Caldicott Guardian should also be encouraged to work with Caldicott Guardians and Senior Information Risk Owners in other organisations, for example to help manage conflicts of interest.

8. A Caldicott Guardian manual has been developed to support Caldicott Guardians and the Caldicott function in this evolving role. Organisations should ensure that Caldicott Guardians and Caldicott Leads are offered effective training and support.

The National Register of Caldicott Guardians

9. NHS and Social Care Caldicott Guardians are 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.

10. To update your organisation’s details on the register, please complete the appropriate certificate for your organisation-type.

11. IMPORTANT: Please return the certificate by post, (not fax, email or scan) to the address stated on it. A hardcopy is required, as the team that manage the register require an original document to provide the sample signature which will be used to authorise people across health and social care to access personal identifiable data and the sensitive data held within computer systems provided by NHS Digital.

12. Please note for NHS organisations, the certificate MUST be countersigned by the organisation's Chief Executive. For Commissioning Support Units (CSUs) it must be countersigned by NHS England’s Caldicott Guardian or an NHS England board member.

13. Details on Caldicott Guardian Council available on https://www.ukcgc.uk/

Caldicott function – key responsibilities

14. The key responsibilities of the Caldicott function are to:

    a. support the Caldicott Guardian;

    b. ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented;

    c. ensure compliance with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training;

    d. contribute to standard one of the Data Security and Protection Toolkit, contributing to the annual assessment;

    e. provide routine reports to the senior management on confidentiality and data protection issues;

    f. identify and address any barriers for sharing for care.

Caldicott Guardians – social care providers

It is not mandatory for social care providers to appoint a registered Caldicott Guardian, though they may choose to do so if this makes sense for their organisation. There should be somebody at a high level within the organisation – which might be the IG Lead – who takes responsibility for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately.

The Caldicott Guardian manual can be a useful resource to assist in this job role and the Caldicott Guardian Council can provide help and guidance:

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

The Role of the Senior Information Risk Owner (SIRO)

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

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

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

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

5. The key responsibilities of the SIRO are to:

    a. Oversee the development of an Information Risk Policy, and a strategy for implementing the policy within the existing Information Governance framework.

    b. Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk

    c. Review and agree action in respect of identified information risks.

    d. 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.

    e. Provide a focal point for the resolution and / or discussion of information risk issues.

    f. Ensure the board is adequately briefed on information risk issues.

    g. Ensure that all care systems information assets have an assigned Information Asset Owner.

The Senior Information Risk Owner – social care providers

The SIRO is responsible for managing information risks. In small organisations, this might be part of a combined role as noted above. If the organisation appoints an IG Lead who is not part of the senior management team or board, then there should be a SIRO who they report to at the highest level of the organisation.

Data Protection Officer

Extract from the IGA - THE GENERAL DATA PROTECTION REGULATION: GUIDANCE ON THE ROLE OF THE DATA PROTECTION OFFICER

https://digital.nhs.uk/media/35501/IGA-Guidance-on-the-GDPR-DPO-V1-FINAL/pdf/IGA_-_Guidance_on_the_GDPR_DPO_V1_FINAL

1. Health and social care organisations that are public authorities must appoint a Data Protection Officer (DPO).

2. Public authorities include:
    a) General Practices and other providers of NHS funded primary care services
    b) NHS Trusts and Foundation Trusts
    c) health commissioners
    d) local authorities
    e) arm's length bodies.
3. Other controllers or processors must also appoint a DPO where they EITHER: a) process special categories data on a large-scale, OR b) perform regular and systematic monitoring of data subjects on a large-scale.
4. This is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR.
5. Organisations are responsible for making sure that the DPO is provided with adequate resources.
6. Organisations must have procedures in place to make sure that the DPO is consulted on all data protection matters at an early stage (as part of privacy by design and default).
7. Organisations must ensure that the DPO role is independent, free from conflict of interest and reports directly to the highest management level of the organisation – there are specific roles that the DPO cannot perform in conjunction with this new role (see the EU guidelines mentioned at 4.1).
8. The DPO must have expert knowledge of data protection law and practices and the ability to acquire detailed understanding of the organisation's business, the purposes for which it processes, or intends to process personal data.
9. A DPO may be directly employed by an organisation or appointed as an external consultant.
10. A single DPO may be appointed by a group of organisations, provided all of the criteria for the role are met and provided the DPO is easily accessible from each organisation. A DPO team with a nominated contact for each organisation is acceptable. In cases of several public authorities, a single DPO may also be designated, taking into account their organisational structure and size.

Advice on Data Protection Officers for social care providers

The EU General Data Protection Regulations (GDPR) will become applicable in UK Law from 25 May 2018. While the GDPR will not be directly applicable post-Brexit, the Data Protection Bill (which will become the Data Protection Act 2018) will ensure continuity with the legislation set out in the GDPR.

This guidance on Data Protection Officers only refers to articles in the GDPR as the Data Protection Bill continues through parliament. It will be updated as more information becomes available.

Do we need to have a Data Protection Officer?

Unfortunately, this is not a simple yes or no answer.

GDPR says that you must appoint a Data Protection Officer (DPO) if:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

If your organisation is considered a public body under the Freedom of Information Act (e.g. Local authority owned care homes), then you must have a DPO.

For everyone else the advice is less clear.

Why is there no clear answer?

The issue is what is meant by “processing on a large scale of special categories of data”, as the GDPR does not define what is meant by large scale.

The Care Provider Alliance is liaising with the Information Governance Alliance and the Information Commissioner’s Office to find an answer on this topic.

Early indications suggest that social care providers will probably need access to a DPO – though this individual does not need to sit within the organisation. The CPA is continuing discussions and will update you as more information becomes available. The requirements for who can be a DPO are quite strict and it is unlikely that most small providers will have someone who can take on this role internally. The CPA are looking into where this resource might be found.

What should I do now?

Continue to check this guidance which will be updated.

Assign someone in your organisation to take on a “champion” role who is responsible for data security and data protection – this might be the individual who is your Information Governance Lead. This individual should familiarise themselves with data security and data protection topics. A good first step would be to complete the e-learning.

Skills for Care and others are putting together core competencies for the champion role. We will update once more information becomes available.

The role and characteristics of a DPO

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

The DPO’s responsibilities include:

1) Informing and advising organisations about complying with GDPR and other data protection laws.
2) Monitoring compliance with GDPR and data protection laws – including staff training and internal audits.
3) Advising on and monitoring data protection impact assessments.
4) 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 many social care 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 registered manager plans to bring in a new rota system which would include staff personal details; they could not also be the DPO because the decision-making process might conflict with data protection obligations.

If you decide you need a DPO or volunteer to appoint a DPO

There is more information about requirements for DPOs here:

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

If you decide that you do not require a DPO

If you decide that your organisation does not require a DPO, you should document your reasons why you do not believe you need to appoint someone in this position.