Data Security and Protection Responsibilities

It is really important that you have people in your organisation who take responsibility for data security and protection.

The Data Security and Protection Toolkit (DSPT) asks that you have 4 different roles for this. However, you can combine these roles or you can decide that there isn't a requirement for your organisation to have someone in this role. There is also no need to use these job titles as long as someone is taking on these responsibilities.

This guide will give you a brief overview of the roles – there is more in-depth information, including job characteristics in the Key Roles and DPO guide (this document covers all sectors, so make sure that you read the social care sections).

Information Governance (IG) Lead / Data Protection Champion

This is the person who will be co-ordinating your data security and protection work. This doesn't need to fall on the Registered Manager's shoulders but should be someone who has enough seniority in your organisation that they can fulfil their responsibilities. Equally, this could be a role which is shared between several staff members.

This role is referred to as the IG Lead in the DSPT. We refer to this role as the Data Protection Champion throughout our materials to match the job description which has been developed by Skills for Care.

It is likely that the person(s) who is completing the DSPT will be your Data Protection Champion. This role could be job shared.

Senior Information Risk Owner (SIRO)

The SIRO should be someone at board or senior management level who can lead on data security and protection from the very top of the organisation. The SIRO's key responsibility is to manage information risks and to provide leadership and guidance from a senior level. This could be a combined role with the Data Protection Champion.

Caldicott Guardian

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

It is mandatory for all NHS organisations and Local Authorities providing social services to have a Caldicott Guardian who is publicly registered on the National Register of Caldicott Guardians. Other health and care organisations (e.g. from the independent sector) are encouraged to register a Caldicott Guardian but this is not mandatory.

There needs to be someone within your organisation who is looking after people's information rights – this could be a combined role with the Data Protection Champion.

Data Protection Officer (DPO)

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

- are a public authority[1] (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[2] 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. You should discuss with your CCG or LA about how to access to a DPO.

We advise that large social care providers are likely to need to appoint a DPO as part of their journey towards compliance. A large care organisation could be characterised as multisite (perhaps on a regional or national level) with dedicated staff in roles such as IT, HR and estates. They have large volumes of care records.

[1] This is defined in the Freedom of Information Act 2000 and will only apply to NHS or LA owned care providers.
[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.

There is guidance on this role in the Key Roles and DPO guide. Skills for Care have developed more guidance on if you need someone in this role and what their responsibilities will be here.

For smaller care providers, you should appoint somebody in a champion role (see above). A small care provider could be characterised as having one or two sites, no dedicated staff in roles such as IT or HR and a small volume of care records.

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. 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.