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 assign responsibility for data security and protection to someone in your organisation i.e. an Information Governance (IG) Lead. We have called this person a Data Security and Protection Lead. Their responsibility is to provide leadership and guidance from a senior level.

This guide will give you a brief overview of what the responsibilities of this person are. At the end we also cover the role of a Data Protection Officer (DPO) and a Caldicott Guardian, these specialist roles are not required for all care providers.

Data Security and Protection Lead (IG Lead)

This is the person who takes overall senior responsibility for 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. Elements of this role could be shared between more than one person. For example, in large organisations there may be one senior person responsible for managing risks and another responsible for information governance.

Skill for Care have developed a job description for this role (This opens a PDF).

The core role of the Data Security and Protection Lead is to champion data security and protection good practice and ensures that it is implemented.

It is important that the lead has good knowledge and skills around data security and protection. We recommend that the Data Security and Protection Lead completes e-Learning for Healthcare's Data Security Awareness training or equivalent.

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. You can find out what the role entails by reading the Caldicott Guardian Manual.

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. **It is not mandatory** for other health and social care organisations (e.g. from the independent sector) to appoint a registered Caldicott Guardian, though they may choose to do so if this makes sense for their organisation. In small organisations, the Data Security and Protection Lead might take on the responsibilities of the Caldicott Guardian function i.e. protecting the confidentiality of peoples' health and care data and making sure that it is used appropriately.

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 Local Authority about how to access a DPO.

[1] This is defined in the Freedom of Information Act 2000 and will only apply to NHS or Local Authority 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.

We advise that large social care providers are likely to need to appoint or have access to a DPO. 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.

The DPO is responsible for advising the organisation about data protection laws and monitoring compliance. They should have expert knowledge of data protection law and practices, and understand the organisation's business, and be independent i.e. they cannot receive instructions on how to carry out their tasks relating to data processing. 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. Skills for Care have developed more guidance on whether or not you need a DPO and what their responsibilities are here (This opens a PDF).

Smaller care providers do not need to appoint a DPO and can have a Data Security and Protection Lead instead (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 the lead person as a Data Protection Officer as a DPO has specific legal requirements. The lead person 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.

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 Security and Protection Lead. **It is not mandatory** for social care organisations to appoint a SIRO.