

# Data Security and Protection Toolkit

## Organisation profile questions – guidance for social care organisations

Question	Guidance
<b>Please enter key role details for Caldicott Guardian.</b>	<p>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 to have a Caldicott Guardian who is publicly registered on the National Register.</p> <p>It is not mandatory for other health and social care organisations (e.g. from the independent sector) to have one, but there needs to be someone within your organisation who is looking after people’s information rights. In small organisations, the Information Governance Lead or 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. Read more about the Caldicott Guardian role in <a href="#">Key Roles and DPO Guide (opens in a new tab)</a>.</p> <p>If you have a Caldicott Guardian, enter their name and email address, otherwise leave this question.</p>
<b>Please enter key role details for SIRO.</b>	<p>The Senior Information Risk Owner (SIRO) is someone at board or senior management level who is responsible for information risks and provides leadership and guidance from the top of the organisation. Read about the SIRO in the <a href="#">Key Roles and DPO Guide (opens in a new tab)</a></p> <p>For small organisations this could be a combined role with the Information Governance Lead or Data Security and Protection Lead. Advice on these roles for social care providers can be found at Digital Social Care in <a href="#">Data Security and Protection Responsibilities (opens in a new tab)</a></p> <p>If you have a SIRO, enter their name and email address, otherwise leave this question.</p>

<p><b>Please enter key role details for IG Lead.</b></p>	<p>The Information Governance (IG) Lead is the person who takes overall senior responsibility for information governance in your organisation. They are likely to be responsible for ensuring completion of this Toolkit - or to assign responsibility for completing the DSPT.</p> <p>In social care organisations this role is sometimes called the Data Security and Protection Lead to match the job description which has been developed by <a href="#">Skills for Care</a>. In small organisations this role could be shared between more than one staff member. The 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. Advice on the Data Security and Protection Lead role for social care providers can be found at Digital Social Care in <a href="#">Data Security and Protection Responsibilities (opens in a new tab)</a></p> <p>Enter the name and email address of your Information Governance / Data Security and Protection Lead.</p>
<p><b>Please enter key role details for Data Protection Officer.</b></p>	<p>You must appoint a Data Protection Officer (DPO) if you are a public authority. Public authorities include local authorities, NHS Trusts and Foundation Trusts, General Practices and other providers of NHS funded primary care services. Read more about the DPO role in <a href="#">Key Roles and DPO Guide (opens in a new tab)</a></p> <p>Other types of organisations only need to have a DPO, or have access to a DPO, if they undertake 'large scale' processing of special categories of data e.g. they have large volumes of health or care records. Otherwise they could have somebody in an Information Governance Lead or Data Security and Protection Lead role instead. Advice on DPOs and these roles for social care providers can be found at Digital Social Care in <a href="#">Data Security and Protection Responsibilities (opens in a new tab)</a></p> <p>If you have a DPO, enter their name and email address, otherwise leave this question.</p>
<p><b>Is NHSmail the only email system used by your organisation?</b></p>	<p>NHSmail (also known as NHS.Net) automatically provides the security required for some of the evidence items in this Toolkit.</p> <p>Select "No" if you do not use NHSmail, or if you use another email system as well as NHSmail. You can select "Not Sure" if you do not know the answer to this question.</p>

<p><b>Does your organisation have Cyber Essentials PLUS Certification, with a scope covering all health and care data processing, awarded during the last 12 months?</b></p>	<p><a href="#">Cyber Essentials PLUS Certification (opens in a new tab)</a> is not mandatory, but having it means that you have the right security in place for some of the evidence items in this Toolkit.</p> <p>If you have the award, select “Yes” and upload your Cyber Essential Plus certificate. You can select “Not Sure” if you do not know the answer to this question.</p>
--	--