The Caldicott Principles

What is Caldicott?

In 1997, a report about confidentiality was produced by a committee chaired by Dame Fiona Caldicott. Their brief had been to review the transfer of person identifying information in the health service. The result was a set of standards that became known as the Caldicott Principles.

Within Health and Social Care, staff may, according to their role, be required to have access to different types of information or ‘data’. This information is often about people (such as service users/patients, carers, colleagues, relations of service users and the like), and may be in many forms (such as written, on computer or verbal).

The Caldicott Principles govern the use of information about service users to ensure that the minimum amount of person identifiable information is exchanged, and only when absolutely necessary. A service user is defined as an individual who is in receipt of services provided either by Devon Social Care, its partner organisations or other agencies. To make sure that all Health and Social Care Organisations are adhering to the Caldicott Principles, a Caldicott Guardian in senior management is appointed to oversee all matters to do with privacy and confidentiality.

The Devon County Council Caldicott Guardian is Tim Golby, Head of Social Care Commissioning.

Confidentiality is not some ideal to strive for. It is part of the day to day activity of all staff that have access to and use person identifiable information and must be rigorously observed in order to deliver a seamless provision of care.

Caldicott is related to and is supported by other legislation:

3. The common law duty of confidentiality derived from case law rather than statute. This provides individuals with a qualified right to prevent unauthorised disclosure of information concerning them when it was provided in confidence.

Together with the above legislation, the seven Caldicott Principles – see table below - form the basis of best practice in information management. They also allow for the secure transfer of sensitive information amongst professionals within the social care service and across partner agencies.

What is Person Identifiable Information?

The Caldicott Committee identified key items of information, which could be used to establish the identity of a service user:

1. National Identifier, for example, the National Insurance Number or NHS Number.
2. Local Identifier, for example, a System Reference number.
3. Name.
4. Address.
6. Date of Birth.
7. Other Dates, such as Date of Death.
8. Sex.
10. Occupation.
11. Information that relates to a service user, which can be used to identify them, for example, the name of their advocate.
12. The information in question and other information held, or are likely to hold.
13. Any expression of opinion about the service user.
14. Indications of individuals’ intentions in respect of the service user (that is if a connection can be made between the information in question and the service user).
15. Images of the service user, for example, via a CCTV camera.
16. An e-mail address, where its format is sufficient to carry enough detail about a service user, (for example, joe.bloggs@hotmail.co.uk.).
17. Any combination of information that could lead to the identification of a service user(s), (for example, a street name and surname).
### The Caldicott Principles for handling Person Identifiable Information

<table>
<thead>
<tr>
<th>Principle</th>
<th>Your responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Justify the purpose for needing the information. (This includes collecting, dealing with, disseminating, and disposing of person identifiable information).</td>
<td>Every proposed use or transfer of person identifiable information made by staff members must either be required of their role or must be responsibilities that they have been expressly authorised to carry out. The tasks and responsibilities of each individual will be clearly explained in detail, as part of the staff induction process.</td>
</tr>
<tr>
<td>2. Do not use person identifiable information unless it is absolutely necessary.</td>
<td>Person identifiable information items should only be used when there is no alternative. The Social Care identification number should be used instead of name, address and date of birth wherever possible.</td>
</tr>
<tr>
<td>3. Use the minimum amount necessary of person identifiable information.</td>
<td>Where use of person identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.</td>
</tr>
<tr>
<td>4. Access to person identifiable information should be on a strict need to know basis.</td>
<td>Only those individuals who need access to person identifiable information should have access to it, in order to undertake tasks within their job role, or tasks which they have expressly been given responsibility for.</td>
</tr>
<tr>
<td>5. Everyone should be aware of their responsibilities.</td>
<td>Action should be taken to ensure that staff handling person identifiable information are aware of their responsibilities and obligations to respect an individual’s confidentiality.</td>
</tr>
<tr>
<td>6. Everyone should understand and comply with the law.</td>
<td>Every use of person identifiable information must be lawful.</td>
</tr>
<tr>
<td>7. The duty to share information can be as important as the duty to protect patient confidentiality</td>
<td>Staff should have the confidence to share information in the best interests of their clients within the framework set out by these principles, supported by the policies of their employers, regulators and professional bodies.</td>
</tr>
</tbody>
</table>