

Information sharing for social care employers

Ciarán Morrison; Laura Rooney

Document reference number	DHI+DDMMYY+doctype+000X <i>DHI270117S0011</i> <ul style="list-style-type: none"> ○ E = exploratory report ○ L = lab report ○ F = factory report ○ S = summary document ○ LR = literature review ○ RR = research report ○ MR = market research ○ MAP = mapping ○ V=video ○ O= other
----------------------------------	---

Publication date	27/1/2017
Revision date	
Revision number	

Purpose of document	Summary of digital skills related document
Other detail (delete row if appropriate)	

Related projects	Names and doc reference numbers
Keywords	Digital skills; social care; information management

Information sharing for social care employers

Skills for care 2015

Government policy has outlined the importance and increasing need for information sharing between organisations at a local level. Everyone working in health and social care should see the use and safe sharing of information as part of their responsibility.

Why do I need to share information with other agencies?

The publishing and acceptance of the Caldicott Report provides an understanding that social care employers and other partners have a legal duty to share information appropriately. Planning for future services, giving excellent information, advice and guidance all depend to some degree on the pooling of data and information across areas and between partners. Aside from the legal requirements, there are benefits to sharing information and data which include:

- Making sure the right people are involved in offering the right help to the right people
- With an emphasis on prevention and wellbeing, it is vital services share information effectively
- Integrated care is seen as being increasingly important, this cannot be delivered without effective information sharing
- Professionals can work together more efficiently
- Effective information sharing can lead to more efficient use of resources
- Ensures proper safeguarding
- Individuals expect organisations to share information, to avoid repeating themselves
- The failure to share information correctly can have devastating impacts on individuals

What are Caldicott Guardians?

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of individuals using care and support services enabling appropriate information sharing. The guardian acts as the conscience of an organisation and actively supports work that enables information sharing when appropriate. Organisations, such as local authorities, with adult social care and public health responsibilities and commissioned services where the commissioner requires a Guardian, including trusts, Clinical

Commissioning groups, strategic health authorities and special authorities. Not all social care organisations will have or be required to have a Caldicott Guardian.

What are Caldicott Principles?

1. Justify the purpose sharing information
2. Don't use individual's identifiable information unless it is necessary and ensure its accuracy
3. Use minimum necessary individual-identifiable information; making sure information is relevant and not excessive
4. Access to individual identifiable information should be aware of their responsibilities
5. Understand and comply with the law remembering that information shouldn't be transferred to countries outside the EEA or countries without adequate protection until suitable arrangements are in place
6. Understand and comply with the law remembering that information shouldn't be transferred outside of the EEA or countries without adequate protection
7. The duty to share information can be as important as protecting confidentiality, this shifts the balance for social care employers away from not sharing information to emphasise the responsibility to share when appropriate

Data and information security

It's vital to have systems, processes and behaviours that ensure individuals information and data is kept safely. Social care employers should consider how their staff contribute to this.

How do I know what information to share?

One of the first things that employers ask is what information should I be sharing? There is no one answer, though part of the answer will be created locally by understanding what benefits could be possible by sharing certain types of data or information. Not all information needs to be shared and we need to clearly justify the reasoning behind sharing information.

Some questions that might be helpful for kick starting this process of understanding your purpose include:

- What is the specific purpose of the information you wish to share?
- How will collecting it contribute to better outcomes for individuals?
- How will sharing it contribute to better outcomes for individuals?

- Who else would benefit from this process as well as individuals (what other services or bodies could make efficiencies or improve responses via the use of this information?)
- Who potentially has the information you want? Who are the partners/stakeholders?
- Have you begun to think about how you will gain consent from individuals to share information?
- Have you begun to think about how you will deal with objections to information sharing from individuals?

How do I implement change?

The major challenge of any implementation of change is securing a new way of working from the workers on the ground. You may want to ask the following questions:

- Are existing recording practices and procedures good enough to enable the information to be shared?
- Who needs to know about changed procedures?
- Who is the priority group?
- Do they already have a good knowledge of data protection or do we need to go 'back to basics'?
- Have the policies been tried and tested with practitioners and do they make sense 'on the ground'?
- What plans do we have to equip staff to talk confidently to individuals to gain their consent and understanding?
- Is it clear where responsibility for compliance and decision making lies within 'front line' teams?
- Are staff clear on confidentiality issues?
- Is it clear how staff can obtain advice and guidance if they are not clear?
- Is it clear how our policies relate to safeguarding responsibilities?
- Is there an easy visual or booklet to remind staff of the steps involved?
- Are we sufficiently skilled and equipped in basic computer / information security?
- What steps should we take to make sure our data is safe?