The CARE CERTIFICATE

Handling Information

- What you need to know

Standard 14

Handling Information

Confidentiality is a very important right of individuals who receive care and support. It is part of the relationship of trust that individuals have with healthcare support workers and adult social care workers.

Information should always be shared on a need-to-know basis only - for example, with other workers involved in the individual's care. You should not share information with anybody else, even the person's family or friends, without the individual's permission. For example, an individual may not want a friend to know about their health or if they have been unhappy. It is also essential to protect private information from accidental viewing or hearing. For example, if you met another worker and chatted about your work you should consider whether others would be able to hear or if a personal letter to an individual was left in a public place where other people could read it.

Today there are ways of keeping in touch with people, for example, Facebook and Twitter, where information is shared instantly. As a health or social care worker you should be careful to use these responsibly and be mindful of the confidentiality rights of all individuals including other workers. Many workers have mobile technology with them at work which means it is possible to share information about their day or individuals without enough thought and so there are increased risks of breaching confidentiality. This is just as much a breach as leaving a record out of the filing system or remaining logged in to a computer when you are not present. Breaching confidentiality through use of social media, including taking or sharing photos or videos, may be a disciplinary offence, and in some cases may even be a criminal offence depending on what is shared.

Overall, you have a responsibility as a health or social care worker to safeguard an individual's personal information. You should also treat personal information about other workers that you have access to in the same way. Your employer must have systems in place to meet the legal requirements about storing information and you must act within your employer's agreed ways of working. Ask your employer to talk you through the system in use in your workplace to protect information.

Agreed ways of working

Agreed ways of working are an organisation's policies and procedures. This includes those less formally documented by individual employers and the self-employed as well as formal policies.

Legislation

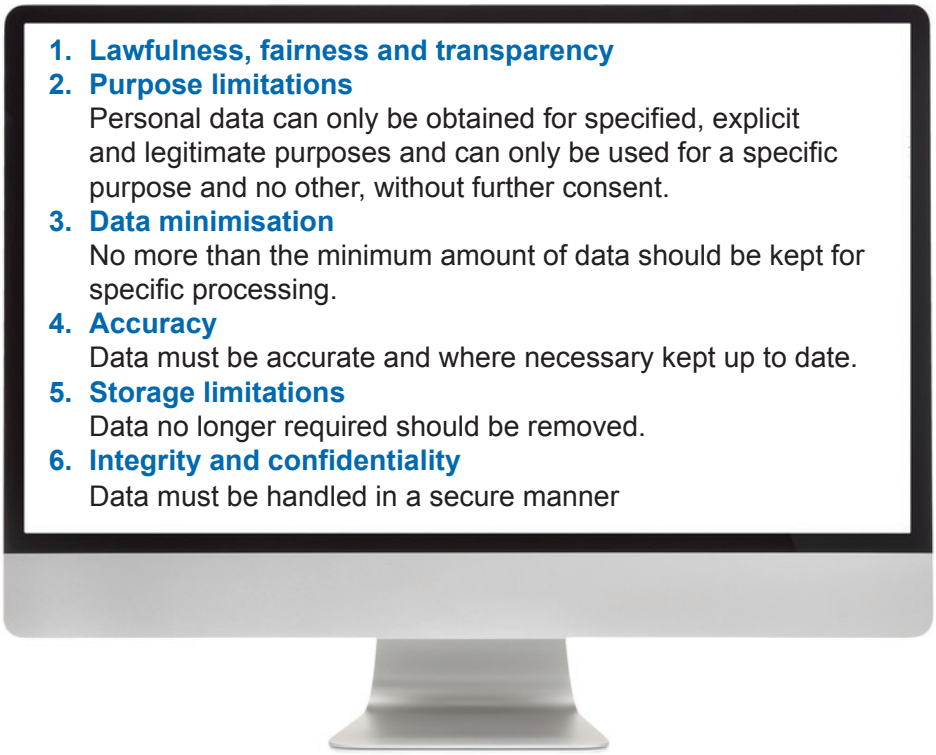
Increasingly, personal information is stored in computer databases. The General Data Protection Regulation (GDPR) 2016 regulates the use of this information ('data') to balance the individual's right to confidentiality and an organisation's need to use it.

The General Data Protection Regulation (GDPR) 2016 replaces the Data Protection Act 1998. This covers any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. It also introduces 'digital rights' for individual citizens. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Legislation

Legislation is laws and the government guidance on the legal rules that affect people in society.

There are 6 privacy principles contained within the GDPR:



The Freedom of Information Act 2000

There is a right under the Freedom of Information Act and the Environmental Information Regulations (EIR) to request information held by public authorities. This came into force in January 2005 and is known as 'the right to know'. It allows you to access recorded information (such as emails, meeting minutes, research or reports) held by public authorities in England, Northern Ireland and Wales.

Under the Act, 'public authority' includes:

- central government and government departments
- local authorities
- hospitals, doctors' surgeries, dentists, pharmacists and opticians
- state schools, colleges and universities
- police forces and prison services.

If you work within an organisation where this applies, please note that individuals have the right to view anything written about them. This may include documents, reports and even emails between two co-workers. This means that if you add to any of these records you need to remember that what you write must be accurate and suitable to be viewed by those whom it concerns. If a public authority believes that the information is covered by a qualified exemption or exception, it must apply the 'public interest test'. This means it has to identify the reason why it is not in the public interest for that information to be shared. ('Public interest' does not mean that the public might find it interesting; it means that there is good reason for something to be made public.) You can find more information here: www.gov.uk/make-a-freedom-of-information-request/the-freedom-of-information-act

Handling information in health and social care

Your employer will have agreed ways of working in place to protect information. Those in relation to electronic information will include having a computer firewall and password protection. Passwords should only be shared with those who have permission to access the information concerned. If you have a personal password to access information at work, you should not share it with anyone else or allow it to be found by anyone. There will also be practices related to paper-based systems, such as where they are kept and the procedure for access. Even when providing care and support in someone's own home it is important to know what records there are and where they are kept. Ask your manager to explain your agreed ways of working about handling information and to answer any questions you may have.

Digital working, digital learning and digital information sharing are becoming everyday practice in health and social care. There is increased understanding of the benefits of improved communication and access to a wide range of knowledge. It is now an aspiration that everyone delivering care and support will have the confidence to work digitally and the opportunity to develop their digital skills, whether with computers, smart phones or **assistive technology**.

Assistive Technology

Assistive technology is any technology that can be used to improve the functional independence of a person with a disability

Care plans

Care plans are a key record about an individual's needs and choices and include assessment of risks. They are an important tool in good communication between those who are involved in providing care and support. Ask your employer to share examples of care plans with you, talking you through how they are completed and what information should be included. They must always be kept up to date, complete, accurate and legible in order to ensure quality and consistency of **care**. They may become legal documents of evidence if at any point there is cause for concern or an enquiry. It is therefore vital you include all details of the agreed care, as well as writing tidily and in a way that is clearly understood, avoiding jargon, and ensuring that the information is factual and not based on opinion. Someone in your workplace will have the responsibility for checking care plans regularly to ensure they are fit for purpose.

6Cs

Care

Care is central to work within the social care and health sectors and must always take account of the individual's wellbeing needs.

Reporting concerns

There might be times when you have concerns over the recording, storing or sharing of information. These could be to do with bad practice relating to confidentiality—for example, if files containing sensitive information have been left lying around or the key for the office has gone missing. Or, they could be to do with how to handle information about risks to the wellbeing of an individual. In either case your manager would be your first port of call.

Managers must be told immediately about any concerns over breaches of confidentiality so they can take action. For example, if files have been left lying around for any unauthorised person to see, the manager must speak to the worker who took them out, remind all staff of the agreed ways of working, inform the person to whom the record relates and take any action possible to limit the damage caused. If a key has gone missing there need to be checks to see that nothing has been improperly removed and the locks need to be changed.

Health and social care workers have a duty to report unsafe or incompetent practice to their organisation's regulatory body—for example, the CQC. If the manager doesn't take your concerns seriously it is your responsibility to make the report under the whistleblowing procedure. If your concerns are based on an individual's information you will need to obtain their permission before making a complaint. Whenever you have major concerns about the recording, storing or sharing of information, you should make a written record, stating your concerns and who you have reported to. You should sign and date it as it might be used as evidence, at a later stage, that you reported your concerns properly.

6Cs

Courage
Courage gives us the confidence to do the right thing in difficult or challenging situations.