Requirements for Registrants on Information Sharing and Data Confidentiality

This this document should be read in association with the JCCP/CPSA Code of Practice (2023) and with the Confidentiality NHS Code of Practice (2023)

Sharing information, for example as part of a shared care arrangement, is central to safe and effective practice. However, Registrants must have arrangements in place to share information only when required and to protect confidentiality when it is not.

Key Principles

The guidance provided in this document builds on these principles:

You should:

- take all reasonable steps to keep information about service users/clients safe;
- make sure you have the service user's consent if you are passing on their information (unless there are good reasons not to, for example, it is necessary to protect public safety or prevent harm to others;
- obtain explicit consent, in writing, if you are using identifiable information for reasons which are not related to providing care, treatment or other services for them;
- only disclose identifiable information if it is necessary, and, when it is, only disclose the minimum amount necessary;
- advise service users/clients when you have disclosed their information (if this is practical and possible);
- keep appropriate records of disclosure;
- act in accordance with relevant legal requirements and good practice;
- if appropriate, ask for advice from colleagues, professional bodies, unions, legal professionals or from the JCCP; and:
- make your own informed decisions about disclosure and be able to justify them.

Confidentiality and the law

You have a professional and legal responsibility to respect and protect the confidentiality of service users at all times. It is a professional responsibility because the standards as set out in our Code of Practice (2023) are there to protect members of the public and advise that you should protect the confidentiality of service users at all times. Breach of confidentiality issues can affect your registration status with the JCCP.

It is a legal responsibility because of the principles set by law, which say that professionals have a duty to protect the confidentiality of the people they have a professional relationship with. The law also says how you should keep, handle and disclose information.

This guidance document draws on relevant laws that affect health and care professionals and their service users/clients. You must keep up to date with and meet your legal responsibilities. We also refer you to guidance produced by other organisations, such as professional regulatory bodies, which may apply to you. If you are employed, your employer is also likely to have policies about confidentiality and sharing information. You should keep up to date with and follow any guidance or policies that are relevant to your practice.

JCCP Registrants are also referred to the 'Confidentiality: NHS Code of Practice' (November, 2023) document:

https://assets.publishing.service.gov.uk/media/5a7c13f0ed915d210ade16fb/Confidentiality_-_NHS_Code_of_Practice.pdf

Accessing and using information

'Using' information refers to any way that information is handled. This includes accessing information, as well as disclosing information to third parties and using information in marketing, research or teaching. This guidance document focuses mainly on disclosing or sharing information with other professionals or third parties. However, accessing information (including care records) without good reason, permission or authorisation is considered to be breaking confidentiality, even if you do not then share the information with a third party. You should be sure that you have a legitimate reason for accessing information about service users, for example where you need it to provide care, treatment or other services. For other reasons you are likely to need specific permission from the service user.

The JCCP Code of Practice (2023)

Our Code of Practice advises that all JCCP Registrants must treat information about service users/clients as confidential' and advise that Registrants must keep records/data secure by protecting them from loss, damage or inappropriate access. You must therefore take all reasonable steps to protect information about service users/clients and to keep such information/data safe and protected at all times from unauthorised access.

As a responsible professional, it is important that you act if you become aware that information about a service user has been lost, damaged or inappropriately accessed, or if there might be a risk of this happening. You should always take steps to try to make sure that the problem does not happen again.

The General Data Protection Regulation (GDPR), supported by the Data Protection Act 2018 (DPA) governs how personal data (information), including service user records, should be handled. It outlines a number of data-protection principles.

The Cosmetic Practice Standards Authority provide standards for confidentiality, information governance and data protection and signpost to the relevant resources to assist in meeting these expected standards (CPSA Overarching Standards)

Electronic records

Service user/client records that are held electronically must also be held securely in accordance with locally determined information governance policies and procedures. This means making sure you keep electronic records secure and that they can only be accessed by the appropriate people. You should have an effective system in place for restricting access to the records – for example, personal logins and effective passwords. Registrants should also be aware of evolving cyber security threats and have measures in place to mitigate them.

Fax machines should not be used at any time for the transfer of personal service user/client data.

Making decisions for people who lack capacity

You should encourage the person and allow them to make their own decisions and manage their own affairs as much as possible and develop the skills needed to do so.

The law surrounding making decisions on behalf of a person who lacks capacity varies among the UK countries. In England, Wales and Northern Ireland, the law says you must act in the 'best interests' of service users/clients. This includes giving service users who have capacity enough information to make sure that they are able to decide about whether they will allow you to share their information with other people. Both the Mental Capacity Act 2005 and the Mental Capacity Act (Northern Ireland) 2016 set out what you should consider when making 'best interests' decisions on behalf of someone who lacks capacity. However, you need to balance the best interests of the service user against other duties. If you have a legal duty to share the information or need to share it to protect the public interest, you can share it without the consent of the service user/client. In Scotland, the Adults with Incapacity (Scotland) Act 2000 sets out the principles you must follow when making decisions on behalf of someone without capacity.

Please note that further details regarding 'Capacity and Consent to Treatment' are described in the 2023 JCCP/CPSA Code of Practice document.

Disclosing Information by Law

Sometimes, you may be asked for information directly under the law – for example, if a court has ordered you to disclose the information. You have a legal duty to keep to orders made by the court.

You should tell the service user/client if you have had to disclose information about them by law, unless there are good reasons not to – for example, if telling them would affect how serious crime is prevented or detected. You should also only provide the information you have been asked for and keep a record of this.

You should also be aware that not all requests from solicitors, the police or a court are made under a legal power that means you must disclose information. If disclosure is not required by law, and cannot be justified in the public interest, you must get express consent from the service user.

Requests from service users

Service users/clients have the right to see information you hold about them and it is important that you respect this.

Safeguarding

The JCCP Safeguarding Policy/Guidelines (2025) advise that Registrants must take appropriate action if they have concerns about the safety or well-being of children or vulnerable adults. In these situations, the following apply.

− If you are employed, you should follow local policies and processes for raising a safeguarding concern. This might include informing the local council or the police.

− If you are self-employed and you are concerned that someone has caused harm, or could pose a risk to vulnerable groups, you should refer the matter to the Disclosure and Barring Service, or in Scotland, Disclosure Scotland. You may also want to inform the local council or the police.

Confidentiality and Accountability

As a JCCP Registrant, you are responsible and accountable for the decisions you make, including ones about confidentiality and disclosing information. We expect our Registrants to make informed and reasonable decisions about their practice to make sure that you always respect and protect the confidentiality of service users/clients. It is also important that you are able to justify the decisions you make. You should also ensure you are holding service users' information confidentially and sharing it only where lawful and appropriate.

JCCP November 2025