hcpc health & care professions council

Information for registrants

Confidentiality – guidance for registrants

Contents

Section 1:
About this document

This document provides guidance on some of the issues relating to how health and care professionals handle information about service users. We have written it mainly for our registrants, but it might also be helpful to potential registrants, employers and other people who want to know how we expect professionals to approach issues of confidentiality.

This document is not designed to replace local procedures and is not meant to cover every situation where problems can come up. However, it is meant to help you make informed and reasonable decisions relating to issues of confidentiality, in line with our standards.

If you have any questions after reading this document, please see the 'More information' section on page 20. We also explain some of the terms and phrases we use throughout this document in the glossary on page 21.

Language

In most of this guidance, when we refer to 'service users' we mean patients, clients and other people who are directly affected by the care, treatment or other services that registrants provide. The broad principles set out in this guidance also apply to registrants who provide services to organisations rather than individuals.

In this document, 'you' means a registrant and 'we' and 'our' refers to the Health and Care Professions Council.

Section 2:
Key principles

This guidance cannot cover every situation where problems or challenges about confidentiality might come up. However, you should keep the following principles in mind when handling information. The guidance that follows builds on these principles to explain more.

You should:

– take all reasonable steps to keep information about service users 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 other people);
– get express 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;
– tell service users when you have disclosed their information (if this is practical and possible);
– keep appropriate records of disclosure;
– keep up to date with relevant law and good practice;
– if appropriate, ask for advice from colleagues, professional bodies, unions, legal professionals or us; and
– make your own informed decisions about disclosure and be able to justify them.

Section 3:
About us

We are the Health and Care Professions Council (HCPC). We are a regulator and our main aim is to protect the public. To do this, we keep a register of professionals who meet our standards for their training, professional skills, behaviour and health.

Health and care professionals on our Register are called 'registrants'. If registrants do not meet our standards, we can take action against them. In serious cases, this may include removing them from the Register so that they can no longer practise.

Our registrants work in a variety of different settings and with a variety of different people. In this document, we refer to those who use or who are affected by the services of our registrants as 'service users'.

Who do we regulate?

We currently regulate the following professions.

– Arts therapists
– Biomedical scientists
– Chiropodists / podiatrists
– Clinical scientists
– Dietitians
– Hearing aid dispensers
– Occupational therapists
– Operating department practitioners
– Orthoptists
– Paramedics
– Physiotherapists
– Practitioner psychologists
– Prosthetists / orthotists
– Radiographers
– Speech and language therapists

Section 4: Introduction

Confidentiality means protecting personal information. This information might include details of a service user's lifestyle, family, health or care needs which they want to be kept private.

Service users expect the health and care professionals who are involved in their care or treatment, or have access to information about them, to protect their confidentiality at all times. Breaking confidentiality can affect the care or services you provide, as service users will be less likely to provide the information you need to care for them. Doing this may also affect the public's confidence in all health and care professionals.

This document builds on the principles outlined in section two and provides extra guidance about some of the issues which come up about confidentiality. It builds on the expectations of health and care professionals outlined in our standards of conduct, performance and ethics.

Our standards of conduct, performance and ethics

The following standards of conduct, performance and ethics describe the professional behaviour we expect from you. You must:

1. promote and protect the interests of service users and carers;
2. communicate appropriately and effectively;
3. work within the limits of your knowledge and skills;
4. delegate appropriately;
5. respect confidentiality;
6. manage risk;
7. report concerns about safety;
8. be open when things go wrong;
9. be honest and trustworthy; and
10. keep records of your work.

You can download copies of these standards from our website, or you can ask us to send you a copy. Please see the section 'More information' on page 20.

As our registrants work in a variety of settings and roles, we have written our standards so that they are relevant, as far as possible, to all registrants and all professions. We have also written them in a way that means they can take account of any changes in the law, technology or working practices.

Our standards are flexible enough to allow registrants and employers to take account of local circumstances – such as availability of resources – to develop ways of working that are practical, effective and meet the needs of service users.

We have written this document to help you meet our standards. However, there is often more than one way to do this. As a health and care professional, you need to make your own decisions (based on your own judgement) about the best way to meet our standards, taking account of your own practice and the needs of your service users. If someone raises concerns about your practice, we will take account of any steps you have taken, including following this guidance, when we decide whether you have met our standards.

Section 4: Introduction

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 our standards are there to protect the public and say that you should protect the confidentiality of service users at all times. Confidentiality issues can affect your registration.

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 draws on relevant laws that affect health and care professionals and their service users. You are not expected to be an expert on the law, but you must keep up to date with and meet your legal responsibilities. Where helpful, we have referred directly to specific legislation which covers issues related to handling information, consent and capacity (see section 7 for more information about these).

Apart from the law, there is a large amount of guidance produced by other organisations, such as professional 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.

Accessing and using information

When we refer to 'using' information, we mean any way information is handled. This includes accessing information, as well as disclosing information to third parties and using information in research or teaching.

This guidance 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.

Section 5:
What information is confidential?

Information about a service user can be ‘identifiable’ or ‘anonymised’. By identifiable information we mean any information you hold about a service user that could identify them. You must treat this information as confidential.

Identifiable information can include:

– personal details, such as names and addresses;
– information about a service user’s health, treatment or care that could identify them;
– photos, videos or other images; and
– other information that a service user, family member or carer shares with you that is not strictly related to the care, treatment or other services you provide.

Anonymised information is information about a service user that has had all identifiable information removed from it and where there is little or no risk of a service user being identified from the information available. You may be able to share anonymised information more openly in some circumstances. However, you should always consider carefully what you are sharing and who you are sharing it with.

Section 6:
Keeping information safe

What our standards say

Our standards of conduct, performance and ethics say that:

'You must treat information about service users as confidential' (5.1)

and

'You must keep records secure by protecting them from loss, damage or inappropriate access.' (10.3)

This means that you need to take all reasonable steps to protect information about service users. By 'reasonable steps', we mean that you need to take sensible, practical measures to make sure that you keep the information safe.

For example, you could store paper records in a lockable cabinet or room. If you run your own practice, you could develop a clear policy for your practice and provide training for your members of staff. Or, you might make sure that you avoid having conversations about service users in public areas where other people might be able to hear.

If you are employed by an organisation, your employer will normally have policies and guidelines on how you should store, handle and share information. In most circumstances, following these policies will allow you to meet our standards comfortably. However, you still need to think about your own practice to make sure that you are protecting confidentiality at all times.

As a responsible professional, it is important that you take action 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 tell your employer (if you have one) and 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. You can find more information in annex A at the back of this document and on the Information Commissioner's Office website.

Electronic records

Health and care records are increasingly being held electronically, rather than on paper. We do not provide any specific guidelines about the types or features of computer-based systems which registrants should use.

This is partly because technology changes quickly and we would not want to prevent you from using new technologies. It is also because the type of electronic record system you use will depend on your practice, the type of setting you work in and other factors.

If you are employed, you should follow your employer's policies and procedures for electronic record-keeping and keeping information secure.

If you are self-employed and need to set your own policies and procedures, you must make sure that you continue to meet our standards. 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.

Section 7:
Consent and confidentiality

Identifiable information is disclosed for a number of reasons. It can happen when you refer a service user to another health and care professional or when a service user asks for information to be given to a third party.

It is important that you get the service user's permission, or 'consent', before you share or disclose their information or use it for reasons which are not related to the care or services you provide for them. There are some exceptions to this and we cover these later in this document.

What our standards say

Our standards of conduct, performance and ethics say that:

'You must only disclose confidential information if:

– you have permission;
– the law allows this;
– it is in the service user's best interests; or
– it is in the public interest, such as if it is necessary to protect public safety or prevent harm to other people.' (5.2)

What is consent?

Consent, for the purposes of confidentiality, means that the service user understands and does not object to:

– the information being disclosed or shared;
– the reason for the disclosure;
– the people or organisations the information will be shared with; and
– how the information will be used.

For consent to be valid, it must be **voluntary** and **informed**, and the person giving consent must have the **capacity** to make the decision.

– By 'voluntary', we mean that the person makes the decision freely and without being persuaded or pressurised by professionals, family, friends or others.
– By 'informed', we mean that the service user has enough information to make a decision about whether they give their permission for their information to be shared with other people. (This is sometimes called 'informed consent'.) Service users should be fully aware of why you need to share any information about them, how you will do so, who you will be sharing the information with and how that information will be used. You should also tell them how not giving their permission is likely to affect the care, treatment or services they receive.
– By 'capacity' we mean a service user's ability to use and understand information to make a decision and to tell you that decision. We discuss capacity in more detail below.

There are two types of consent for the purposes of confidentiality – **express consent** and **implied consent**.

– Express consent

This is where you are given specific permission to do something. You need to get express consent if you are using identifiable information for reasons which are not related to the care, treatment or other services you provide for the service user, or in a way which they would not reasonably expect. It is also important to get express consent if a service user has previously objected to you sharing their information with other people. Express consent can be spoken or written.

If the service user has given you their express consent verbally, it is good practice to keep an ongoing, up-to-date record of this in their

Section 7:
Consent and confidentiality

formal record. This might include a summary of your discussions, the outcomes of those discussions and any decisions made. If you are employed, your employer may use consent forms or have other procedures in place.

– **Implied consent**
  This is where consent from the service user is not expressly spoken or written but can be taken as understood, for example because they have agreed to receive treatment, care or other services. If you are using identifiable information to care for a service user or provide services to them, in most circumstances you will have their implied consent. Most service users will understand the importance of sharing information within the multidisciplinary team. If you are not sure whether you have implied consent, you should always get express consent.

The DPA deals with the issue of consent. You can find more information in annex A.

Capacity

You must keep up to date and follow the law in this area. If you are employed you should also take account of your employer's policies and processes. If you are self-employed or unsure about a specific situation, you should speak to your professional body or get legal advice.

Examples of reasons an adult service user might lack capacity include:

– a mental-health condition;
– dementia;
– severe learning disabilities;
– brain damage, for example from a stroke;
– a physical or mental condition that causes confusion, drowsiness or loss of consciousness; and
– the effects of alcohol or drugs.

You should assume that adult service users have sufficient capacity unless there is significant evidence to suggest otherwise.

Children and young people

For children under 16, you may need to get consent from someone with parental responsibility. This could be:

– the child's mother or father;
– the child's legally appointed guardian;
– a person with a residence order for the child;
– a local authority designated to care for the child; or
– a local authority or person with an emergency protection order for the child.

However, some children under 16 can give consent if they can fully understand the information given to them. This is known as 'Gillick competence'.

You should treat young people (aged 16 and 17) in the same way as adults and presume they have capacity unless there is significant evidence to suggest otherwise.

Section 7:
Consent and confidentiality

Making decisions for people who lack capacity

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. This includes giving service users who have capacity enough information to make sure that they are able to make a decision 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. You should:

- consider all the circumstances relevant to the service user, for example the type of mental-health condition or physical illness they have;
- consider whether they are likely to have capacity in the near future and if the decision can be postponed until then;
- involve them as far as possible;
- take account of the beliefs, values, wishes and instructions they expressed when they had capacity; and
- be aware of the views of, for example, their close relatives, carers and guardians.

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. We explain this in more detail later in this document.

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.

1. Any action or decision you take must benefit the person and must only be taken when you cannot reasonably achieve that benefit otherwise.

2. Any action or decision you take should be the minimum necessary.

3. You must take account of the present and past wishes and feelings of the person, as far as possible.

4. You should take account of the views of others who have an interest in the person's welfare.

5. 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.

Section 8:
Disclosing information with consent

In most cases, you will need to make sure you have consent from the service user before you disclose or share any identifiable information.

Working with other practitioners

One of the most common reasons for disclosing confidential information will be when you contact other health and care practitioners. This might include discussing a case with a colleague or referring a service user to another health and care professional.

Sharing information is part of good practice. Care is rarely provided by just one health and care professional, and sharing information within the multidisciplinary team or with other organisations or agencies is often an important way of making sure care can be provided effectively.

Most service users will understand the importance of sharing information with others who are involved in their care or treatment and will expect you to do so, so you will normally have implied consent to do this.

However, when you share information with other colleagues, you should make sure that:
– it is necessary to provide the information;
– you only disclose the information that is relevant; and
– the professional receiving the information understands why you are sharing it and that they have a duty to keep it confidential.

If you decide not to contact other practitioners when you might reasonably be expected to, or if a service user asks you not to, it is important that you keep clear records of this and are able to justify your decision.

If you are concerned about a request someone makes for information – for example, you think the information they have asked for is not relevant – you should contact the person who has asked for the information so they can explain their request. You may also want to get legal advice, or advice from a union or professional body if you are a member.

Other reasons

It is important that you get express consent, in writing where possible, if you plan to use identifiable information for reasons which are not directly related to the service user's care or if they would not reasonably expect their information to be used or shared in that way.

Examples might be where you need information for research, teaching or health and care services planning. In many cases it will be sufficient to use information which does not identify the service user. Where possible, it is better to use this than to use identifiable information. You should consider how much information you need to change or remove to make sure that you are protecting the service user's confidentiality. For example, you should consider whether the area you work in means that it might be possible to identify the service user by their job or by their medical condition.

If you need to use identifiable information, you should explain fully to the service user how you will use their information and whether there are any risks involved in disclosing it. You should make sure that their consent is clearly recorded in their notes.

Sometimes, a third party who is not a health and care professional may ask you for information. This might be a request to send information to an insurance company, government agency or a solicitor. You should make sure that you have express consent to provide any information.

Section 8:
Disclosing information with consent

In these situations, you should also keep a written record of the information you have disclosed and only disclose what you have been asked to. You should also offer to show the service user or provide a copy of any report you write about them for such purposes.

If a service user does not give their consent

You should make sure that you explain to the service user the possible effect of not sharing information about their care or other services you are providing.

If a service user who has capacity refuses to give consent for information to be shared with other health and care professionals involved in providing care, treatment or other services, you must respect their decision, even if it could negatively affect the care, treatment or other services they can receive.

However, if the law says you must disclose the information or it is justified in the public interest to do so, you can do so without the consent of the service user. We explain more about situations like this later in this document.

Section 9:
Disclosing information without consent

There are a small number of circumstances where you might need to pass on information without consent, or when you have asked for consent but the service user has refused it.

If the service user is unable to give their consent

In some circumstances it may not be possible to get consent from a service user to share information. For example, in some emergency situations, they may be unable to communicate or give consent because they are very unwell or unconscious. In other circumstances, they may not have capacity to give consent.

As discussed earlier, whether a service user has capacity will depend on a number of things, including their mental capacity and age. If a service user is unable to give consent, you may have to disclose information if it is in their best interests. We have outlined earlier in this guidance what you will need to consider when deciding whether it is in their best interests.

Also, you may need to share information with those closest to them (such as a carer or family members) so that you or other health and care professionals can decide what is in their best interests. It is also reasonable to assume that they would want those closest to them to be kept informed of their condition, treatment or care, unless they have previously said otherwise.

You should speak to your employer (if you have one) or professional body for further guidance.

Public interest

You can also disclose confidential information without consent from the service user if it is in the 'public interest' to do so.

This might be in circumstances where disclosing the information is necessary to prevent a serious crime or serious harm to other people. You can find out whether it is in the public interest to disclose information by considering the possible risk of harm to other people if you do not pass it on, compared with the possible consequences if you do. This includes taking account of how disclosing the information could affect the care, treatment or other services you provide to the service user.

You should carefully consider whether it is in the public interest to disclose the information. If you are unsure, speak to your manager or employer (if you have one), or your union or defence organisation. You may also want to get legal advice.

You need to be able to justify a decision to disclose information in the public interest (or a decision not to disclose information) so it is important that you keep clear records.

Even where it is considered to be in the public interest to disclose confidential information, you should still take appropriate steps to get the service user's consent (if possible) before you do so. You should keep them informed about the situation as much as you can. However, this might not be possible or appropriate in some circumstances, such as when you disclose information to prevent or report a serious crime.

Section 10:
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 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.

Keep in mind 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 have the right to see information you hold about them and it is important that you respect this.

Safeguarding

Our standards of conduct, performance and ethics say that:

'You must take appropriate action if you have concerns about the safety or well-being of children or vulnerable adults.' (7.3)

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.

Section 11:
Disclosing information to regulators

There are a number of regulators – such as the General Medical Council, the Care Quality Commission and us – who may need you to pass on information to them. In some cases regulators have statutory powers to request information (see 'Identifiable information and fitness to practise' below). This section refers to regulators of health and care professionals, but is relevant to other types of regulators as well.

Reporting your concerns

Registrants are often not sure about passing on identifiable information because they do not know how this information might be used. However, so that regulators can protect the public, it is important that you tell them if you have any concerns about whether a registered professional is fit to practise. This is also related to your duties under our standards of conduct, performance and ethics.

When you tell a regulator about your concerns, you may need to include information about a service user. This might be because your concerns are about the care or services provided to a particular service user or group of service users.

If you need to disclose information about a service user, make sure that the information is relevant to your concerns. You should, if possible, remove all identifiable information, including names and addresses. Where it is necessary to include identifiable information it is good practice to tell the service user and try to get their consent for the disclosure. However, if the disclosure is required in the public interest, identifiable data can be disclosed without consent.

You should keep an appropriate record of any disclosures, giving reasons for disclosing the information and a justification for that disclosure where possible.

You might also want to discuss these matters with your manager (if you have one) or a professional colleague.

If you are not sure whether to tell a regulator, what information to provide, or how they will use the information, you should contact the regulator for more advice.

Identifiable information and fitness to practise

Sometimes regulators make requests for information about service users that they need to help them investigate a registrant's fitness to practise. For example, if we are looking at a complaint about a registrant's record-keeping, we might need to ask for copies of the records so that we can decide whether the professional has met our standards.

Regulators often have powers to require information from people other than the person being investigated. They will sometimes make these requests using 'statutory powers'. These are powers that a regulator has by law to help them in an investigation. You have to provide the information, but it is good practice to tell service users (if possible) when you have disclosed information about them.

You should make sure that you only provide the information the regulator has asked for, and provide anonymised or partly anonymised information when you can.

If we ask for information using our statutory powers, we will put this in writing and explain why

Section 11: Disclosing information to regulators

we are asking for it and how we will use it. Information we use during a hearing will usually have all the identifiable information removed from it, and we will always take appropriate steps to make sure that we protect a service user's confidentiality. The law says we have to handle this information responsibly. For example, we use terms such as 'Service user A' to refer to individuals. We may also hold hearings fully or partly in private when necessary.

Section 12:
Confidentiality and accountability

As a health and care professional, you are responsible and accountable for the decisions you make, including ones about confidentiality and disclosing information.

We feel that you are best placed to make practical decisions, taking account of the way in which you practise. You need to make informed and reasonable decisions about your own practice to make sure that you always respect and protect the confidentiality of service users. It is also important that you are able to justify the decisions you make.

If you are employed by an organisation, they are likely to have policies and procedures in place relating to confidentiality. We expect you to practise in line with these.

If you are self-employed or employ other people, we expect you to put in place policies and procedures to make sure you are holding service users' information confidentially and sharing it only where lawful and appropriate.

However, if you find that the policies and procedures relating to confidentiality in the organisation or service where you work are not suitable or appropriate, or do not allow you to carry out your duties, you should raise your concerns. This might be to your manager or the person with responsibility for data protection where you work, or with another appropriate authority. If you feel that your employer's policy might mean that confidentiality is put at risk, you should contact your union, professional body or us for advice.

Section 13:
More information

If you are not sure about what you should do in a specific situation, consider asking your employer, professional body or independent legal representative for advice.

The **Information Commissioner's Office (ICO)** is the UK's independent authority set up to uphold information rights and has produced guidance which you may find useful: https://ico.org.uk/

We also recognise the valuable role professional bodies play in providing advice and guidance to their members. If you are a member of a professional body, you may find it useful to ask for advice about good practice on confidentiality as it relates to your profession.

In particularly complex situations, you might also consider getting independent legal advice.

Contact us

You can contact us if you have any questions about this guidance or what we expect with regard to confidentiality. However, we cannot offer legal advice. Our contact details are below.

The Health and Care Professions Council
Park House
184 Kennington Park Road
London
SE11 4BU

Phone: +44 (0)300 500 6184

You can download copies of our standards documents and other publications from our website at www.hcpc-uk.org

Glossary

You may not be familiar with some of the terms we use throughout this document, so we have explained them below.

Accountable
As an accountable health and care professional, you will be responsible for the decisions you make and you may also be asked to justify them.

Anonymised information
Information about a service user that has had all identifiable information removed from it, and where there is little or no risk of an individual being identified.

Autonomous
As an autonomous health and care professional, you make your own decisions based on your own judgement.

Court order
An order made by a judge or court for something to happen.

Disclose, disclosure
When information is revealed, released or passed on from one person to another.

Express consent
Specific permission from the service user, given verbally or in writing, to use or share information about them.

Fitness to practise
A professional is fit to practise if they have the training, skills, knowledge, character and health to do their job safely and effectively. We can take action if we have concerns about a registrant's fitness to practise.

Identifiable information
Any information that might identify a service user, for example their name, address or details of their health condition, treatment or care.

Implied consent
When a service user is aware of the possibilities for sharing information and their right to refuse this, but does not object.

Informed consent
When a service user has enough information to make a decision about whether they give their permission for information to be shared with other people.

Professional bodies
Organisations which promote or represent members of a profession. They may also provide guidance and advice, produce curriculum frameworks, oversee post-registration education and training, and run continuing professional development (CPD) programmes.

Public interest
Disclosures of information are made in the 'public interest' when it is necessary to prevent a serious threat to public health, national security, the life of the person concerned or another person, or to prevent or detect serious crime.

Register
A published list of health and care professionals who meet our standards. The Register is available on our website at www.hcpc-uk.org

Registrant
A health and care professional who appears on our Register and meets our standards.

Regulator
An organisation that protects the public by making sure people or organisations keep to certain laws or requirements.

Glossary

Service user
Anyone who uses or is affected by the services of a registrant. This includes patients and clients.

Standards of conduct, performance and ethics
Standards of behaviour that we expect from health and care professionals who are registered with us.

Statutory powers
Certain organisations, such as regulators, have powers under legislation. This sometimes includes the power to ask for information from people.

Third party
Someone who is not the service user, a member of their family or a carer or the professional involved in their care or treatment. This could include another professional or an organisation that has requested information.

Annex A:
Data protection principles

(Plain English Campaign's Crystal Mark does not apply to annex A or its glossary.)

The General Data Protection Regulation (GDPR), supported by the Data Protection Act 2018 (DPA) governs how personal data (any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier), including service user records, should be handled.

GDPR principles

GDPR sets out seven key principles, which are broadly similar to the Data Protection Act 1998 (the 1998 Act):

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability. (This is the most substantial change when compared with the 1998 Act).

Lawful basis for processing

You must have at least one lawful bases for processing personal data:

- **Consent:** the individual has given unambiguous consent and for a specified purpose.
- **Contract:** it is necessary under a contract, or as a prerequisite.
- **Legal obligation**.
- **Vital interests:** it is necessary to protect someone's life.
- **Public task:** it is required in the public interest or for an official function.
- **Legitimate interests:** it is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data.

Consent

Consent is one of the six lawful bases for processing personal data and must:

- be unambiguous;
- involve a clear affirmative action
- be prominent, concise and easy to understand and separate from terms and conditions;
- where explicit, be expressed in words; and
- cover the controller's name, the purposes of processing and the types of processing activity.

Purpose limitation

This principle seeks to make sure you are open and transparent about why you are collecting personal data, and that you use that data in a way the individual reasonably expected you to.

In order to satisfy this principle, you must:

- know why you are collecting personal data, and what you will do with it;
- clearly explain why you are collecting personal data, and what you will do with it; and
- only use or disclose information outside of this purpose if it is lawful or transparent.

Data minimisation

You must make sure any personal data you are processing is:

- adequate (to enable you to discharge the intended purpose);
- relevant (has an appropriate link to that purpose); and
- limited (you don't hold any more information than you absolutely need for that purpose).

Annex A:
Data protection principles

Accuracy
You should take reasonable steps to make sure any personal data you hold is accurate and:

– keep it updated as appropriate;
– correct or erase it as appropriate; and
– carefully consider any challenges to the accuracy of the data.

Storage limitation
You must not keep personal data for any longer than you need it. You should:

– be able to justify how long you keep personal data;
– have a clear policy on retention periods;
– regularly review your data to assess whether it needs to be deleted or anonymised;
– consider requests for personal data to be erased on a case by case basis.

Integrity and confidentiality (security)
You must process personal data securely, and ensure you have:

– undertaken an appropriate risk analysis;
– developed a clear policy; and
– considered both physical and technical data.

Accountability
You are responsible for the way you process and store personal data. You have duty to comply with the principles of the GDPR, and should be able to evidence how you do so.

Where to go for further advice and support
The Information Commissioners Office (ICO) is the leading authority in the UK for data protection. It has a number of helpful resources on its website:

– A Guide the General Data Protection Regulation.
– Health and social care FAQs.
– FAQs or small health sector bodies.

Park House
184 Kennington Park Road
London SE11 4BU

tel +44 (0)300 500 6184
fax +44 (0)20 7820 9684
www.hcpc-uk.org

To request this document in Welsh or an alternative format, email publications@hcpc-uk.org

Publication code: 20080206dPOLPUB (revised October 2018)