Council, 6 July 2017

Consultation on revised guidance on Confidentiality

Executive summary and recommendations

Introduction

The HCPC published the document 'Confidentiality – guidance for registrants' in 2008. This guidance document provides advice to registrants on handling information about service users and other issues relating to confidentiality. It was produced to assist registrants in meeting the standards of conduct, performance and ethics (SCPE), which include requirements related to respecting the confidentiality of service users' information. The revised SCPE were published on 26 January 2016.

A consultation was held between 3 October 2016 and 13 January 2017 on revised guidance on Confidentiality.

The consultation response analysis and revised draft guidance are attached for the Committee's consideration, approval, and recommendation to Council.

The revised guidance retains its focus on the core principles of confidentiality but, following consultation feedback, now also provides further detail on related areas such as capacity, best interests and the Data Protection Act.

The Education and Training Committee considered the consultation response analysis and the draft guidance on 12 June 2017 and suggested some minor changes for clarity. These changes have been made and the consultation response analysis and revised draft guidance are attached for the Council's consideration and approval.

Decision

- The Council is invited to discuss and agree the text of the consultation response analysis document and the draft guidance, subject to legal scrutiny and minor editing amendments.

Background information

- The current version of the document 'Confidentiality – guidance for registrants' can be found on the HCPC website: http://www.hcpc-uk.org/publications/brochures/index.asp?id=164

- The revised SCPE were published on 26 January 2016: http://www.hcpc-uk.org/aboutregistration/standards/standardsofconductperformanceandethics/

- Education and Training Committee, 3 March 2016. Reviewing the guidance on confidentiality. http://www.hcpc-uk.org/assets/documents/10004F38Enc08-Reviewingtheguidanceonconfidentiality.pdf

Resource implications

The resource implications include those associated with publication and launch of the revised guidance. These have been taken into account in departmental work plans for 2016/2017.

Financial implications

The financial implications, including reprinting the guidance document, have been accounted for in budget planning 2016/2017

Appendices

- Appendix 1: Guidance on Confidentiality
- Appendix 2: Consultation on revised guidance on Confidentiality – analysis of the responses

Date of paper

21 June 2017

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. It has been written primarily for our registrants, but 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 to 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 22. We also explain some of the terms and phrases we use throughout this document in the Glossary on page 23.

Language

In most of this guidance, when we refer to ‘service users’ we mean to include 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
- Social workers in England
- Speech and language therapists

Section 4. Introduction

Confidentiality means the protection of 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
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 22.

As our registrants work in a variety of settings and in a variety of different 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 an autonomous health and care professional, you still need to make personal decisions 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.

Confidentiality and the law

Your duty to respect and protect the confidentiality of service users at all times is both a professional and a legal responsibility.

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.

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 of 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, you should be aware that 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. Identifiable information about a service user must be treated as confidential.

This 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.

On the other hand, 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 with whom.

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 it is brought to your attention 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 Data Protection Act (DPA) 1998 is a piece of legislation which governs how personal data, including service user records, should be handled. It outlines a number of data protection principles. You can find more information in annex A and on the Information Commissioner’s Office website.

Electronic records

Health and care records are increasingly being held electronically, rather than in paper form. 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 registrants 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 information security.

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. With regard to electronic records, this means ensuring that the records are kept secure and can only be accessed by the appropriate people. An effective system for restricting access to the records – for example, personal logins and effective passwords – should be in place.

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 with which the information will be shared; and
- how the information will be used.

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

- 'Voluntary' means that the decision is made freely and without coercion or pressure from 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; whom 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 communicate their decision to you. Capacity is discussed in further detail below.

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

- **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 could be spoken or written.

  If you have gained express consent verbally it is good practice to keep a contemporaneous record of this in the service user's formal record. This might include a summary of your discussion, 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 seek express consent.

The DPA also provides a definition of consent. Further information can be found at 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 seek legal advice.

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

- mental health conditions;

- dementia;

- severe learning disabilities;

- brain damage, for example from a stroke;

- physical or mental conditions that cause confusion, drowsiness or a loss of consciousness; and

- intoxication by drug or alcohol misuse.

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, it is likely that you will need to seek 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 concerning 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 provide consent if they have sufficient understanding and intelligence to fully comprehend the information given to them. This is known as ‘Gillick competence’.

Young people (aged 16 and 17) should be treated in the same way as adults in that they should be presumed to have capacity, unless there is significant evidence to suggest otherwise.

Best interests/needs of the individual

When making decisions on behalf of a person who lacks capacity, the law varies among the UK countries.

In England and Wales and Northern Ireland, the law requires you to 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 give their consent for you to share their information with other people.

Both the Mental Capacity Act 2005 and the Mental Capacity Act (Northern Ireland) 2016 set out the factors that should be considered when making 'best interests' decisions on behalf of someone who lacks capacity. In broad terms, 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 the service user is likely to have capacity in the near future and if the decision can be postponed until then;

- involve the service user as far as possible;

- take account of the beliefs, values, wishes and instructions expressed when the service user had capacity;

- be mindful of the view of the service user's close relatives, carers, guardians etc.

However, the best interests of the service user should be balanced against other duties. If you have a legal obligation to disclose the information or it is necessary to share the information to protect the public interest, you can disclose without the consent of the service user. We explain this in more detail later in the document.

In Scotland, the Adults with Incapacity (Scotland) Act 2000 sets out the principles to be followed when making decisions on behalf of someone without capacity:

1. any action or decision must benefit the person and only be taken when that benefit cannot reasonably be achieved without it

2. any action or decisions taken should be the minimum necessary to achieve the purpose

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

4. account should be taken of the views of others with an interest in the person's welfare

5. the individual should be encouraged and allowed to make their own decisions and manage their own affairs as much as possible and to 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.

Liaising with other practitioners

One of the most common reasons for disclosing confidential information will be when you liaise with 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 liaise with other practitioners when you might reasonably be expected to, or if a service user asks you not to do so, 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, if it appears that 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 anonymised or de-identified information. Where possible, it is preferable 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 in which you work 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, you may be asked for information by a third party who is not a health and care professional. This might be a request to send information to an insurance company, government agency or a solicitor. You should take steps to make sure that you have express consent to provide any information.

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 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 diminish 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 share the information, you may do so without the consent of the service user. We explain more about such situations 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 consent

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

As discussed earlier in the guidance, whether a service user has capacity will depend on a number of different things, including their mental capacity and age. If a service user is unable to consent, you may have to disclose information if it is in their best interests. The factors you will need to consider to determine best interests are outlined earlier in the guidance.

Additionally, information may need to be shared with those closest to them (such as a carer or family members) to enable you or other health and care professionals to determine 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 previously indicated 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, you should 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 justified 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 comply with the order.

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 undermine the prevention or detection of serious crime. 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 legal compulsion. 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 rights to access information about them and it is important that you respect service users' rights to ask to see their information.

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:

- 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 have concerns that someone has caused harm, or poses a future risk of harm to vulnerable groups, you should make a referral to the Disclosure and Barring Service, or in Scotland, Disclosure Scotland. You may also wish 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. 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, you should make sure that the information is relevant to your concerns. You should, where possible, remove all identifiable information, including names and addresses. Where it is necessary to include identifiable information, it is good practice to inform the service user and try to seek 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 the fitness to practise process

Sometimes regulators make requests for information about service users that they need to help them in an ongoing investigation about 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 from the individual under investigation. They will sometimes make these requests using ‘statutory powers’. These are powers that a regulator has from legislation 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 we are asking for the information 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. We have a legal obligation 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 an autonomous 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 practice. You need to make informed and reasonable decisions about your own practice to make sure that you respect and protect the confidentiality of service users at all times. 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 accordance with these.

If you are self-employed or employ others, 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 enable you to fulfil 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, you should consider asking for advice from your employer, professional body, or independent legal representative.

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/

In addition we 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 relating to 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 our expectations with regard to confidentiality. Please be aware, however, that 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.

tel +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, e.g. 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 carry out work such as providing guidance and advice, producing curriculum frameworks, overseeing post-registration education and training, and running continuing professional development programmes.

Public interest
Disclosures of information are made in the 'public interest' where they are necessary to prevent a serious threat to public health, national security, the life of the individual 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.

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 derived from legislation. This sometimes includes the power to require 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

The Data Protection Act (DPA) 1998 regulates the processing of personal data and outlines a number of data protection principles. We have repeated these principles in full below. The Information Commissioner's Office (ICO's) website (see section 12) includes helpful information about what these principles mean.

a. personal data must be processed **fairly and lawfully**

b. personal data should be obtained for one or more specified and lawful **purposes** and should not be processed in any manner incompatible with that purpose(s)

c. personal data should be **adequate**, relevant and not excessive in relation to the purpose(s) for which they are processed

d. personal data should be **accurate** and, where necessary, kept up to date

e. personal data should not be kept for longer than is necessary

f. personal data should be processed in accordance with the rights of the data subject

g. appropriate measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

h. personal data should not be transferred to a country or territory outside the European Economic Areas unless there are adequate levels of protection for the rights and freedoms of data subjects in relation to the processing of personal data in that country or territory.

Conditions for processing

In order to satisfy principle one (to process data fairly and lawfully), one or more 'conditions for processing' must be met whenever personal data is processed. These conditions are:

a. The individual who the personal data is about has consented to the processing.

b. The processing is necessary:

    i. In relation to a contract which the individual has entered into; or

    ii. Because the individual has asked for something to be done so they can enter into a contract.

c. The processing is necessary because of a legal obligation (except an obligation imposed by a contract).

d. The processing is necessary to protect the individual's 'vital interests'. This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

e. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

f. The processing is in accordance with the 'legitimate interests' condition.

Sensitive personal data

The DPA outlines additional requirements for the processing of **sensitive** personal data. Sensitive data means personal data consisting of information about an individual's:

a. racial or ethnic origin of the data subject

b. political opinions

c. religious belief or other beliefs of a similar nature

d. whether they are a member of a trade union

e. their physical or mental health condition

f. their sexual life

g. the details of any offence they have committed, or are alleged to have committed

h. any proceedings relating to an offence they have committed (or are alleged to have committed) including any outcome or sentence.

Sensitive personal data should be treated with greater care than other personal data. If you are processing data you must satisfy one or more of the 'conditions for processing' outlined above. You must also meet at least one of the conditions set out below:

a. the individual who the sensitive personal data is about has given explicit consent to the processing

b. the processing is necessary so that you can comply with employment law

c. the processing is necessary to protect the vital interests of:

i. the individual (in a case where the individual's consent cannot be given or reasonably obtained), or

ii. another person (in a case where the individual's consent has been unreasonably withheld)

d. the processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents

e. the individual has deliberately made the information public

f. the processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights

g. the processing is necessary for administering justice, or for exercising statutory or governmental functions

h. the processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality

i. the processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Consent

Consent under the DPA follows the definition set out in the European Data Protection Directive:

'…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

To satisfy this, consent must be:

a. given by some active communication between the parties and should not be inferred (although it doesn't have to be in writing)

b. appropriate to the age and capacity of the individual and to the circumstances of the case

c. clear, covering the type of information, the purposes of processing and any special aspects which may affect the individual

d. timely – consent will not necessarily last forever, although it will usually last for as long as the related processing continues.

For further information about DPA principles, please visit the Information Commissioner's Office website.

Glossary of terms used in annex A

Data controller (as defined by the Data Protection Act 1998)
A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Processing (as defined by the Data Protection Act 1998)
In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. For further information please visit the Information Commissioner's Office website.

Personal data (as defined by the Data Protection Act 1998)
Data which relate to a living individual who can be identified from those data or from those data together with other information which is in the possession of, or is likely to come into the possession of, the data controller.

Consultation on revised guidance on confidentiality

Analysis of responses to the consultation on 'Confidentiality' and our decisions resulting from responses received

Contents

1. Introduction

About the consultation

1.1 We consulted between 3 October 2016 and 13 January 2017 on proposals to revise the guidance on confidentiality.

1.2 The guidance document, entitled 'Confidentiality – guidance for registrants' was first published in June 2008. We have recently reviewed the guidance in order to make sure that it remains up to date and useful for our registrants and other stakeholders. We also want to make sure that the guidance takes account of recent changes to the HCPC standards of conduct, performance and ethics

1.3 We informed a range of stakeholders about the consultation including professional bodies, employers, and education and training providers, advertised the consultation on our website, and issued a press release.

1.4 We would like to thank all those who took the time to respond to the consultation document. You can download the consultation document and a copy of this responses document from our website: www.hcpc-uk.org/aboutus/consultations/closed.

About us

1.5 We are a regulator and were set up to protect the public. To do this, we keep a Register of health and care professionals who meet our standards for their professional skills and behaviour. Individuals on our register are called 'registrants'.

About this document

1.6 To protect the public, we set standards that professionals must meet. Our standards cover the professionals' education and training, behaviour, professional skills, and their health. We publish a Register of professionals who meet our standards. Professionals on our Register are called 'registrants'. If registrants do not meet our standards, we can take action against them which may include removing them from the Register so that they can no longer practise.

1.7 This document summarises the responses we received to the consultation.

1.8 The document starts by explaining how we handled and analysed the responses we received, providing some overall statistics from the responses. Section three provides a summary of the general comments we received, while section four is structured around the responses we received to specific questions. Our responses and decisions as a result of the comments we received are set out in section five.

1.9 In this document, ‘you’ or ‘your’ is a reference to respondents to the consultation, ‘we, ‘us’ and ‘our’ are references to the HCPC.

2. Analysing your responses

2.1 Now that the consultation has ended, we have analysed all the responses we received.

Method of recording and analysis

2.2 The majority of respondents used our online survey tool to respond to the consultation. This invited them to indicate whether they were responding as an individual or on behalf of an organisation. For each question they answered, respondents were able to select from four options: yes; no, partly; and don't know. They were also able to give us their comments on each question in a free text box.

2.3 During the consultation period we held five workshops to seek the views of our education partners about the standards. We recorded the feedback we received and have included it alongside the responses to the consultation.

2.4 Where we received responses by email or by letter, we recorded each response in a similar format.

2.5 When deciding what information to include in this document, we assessed the frequency of the comments made and identified themes. This document summarises the common themes across all responses, and indicates the frequency of arguments and comments made by respondents.

Quantitative analysis

2.6 We received 43 responses to the consultation document. 20 responses (47%) were made by individuals of which 17 (85%) were HCPC registered professionals and 23 (53%) were made on behalf of organisations.

2.7 The table below provides some indicative statistics for the answers to the consultation questions. Responses to question seven, which asked for any other comments on the standards are summarised in section three of this paper.

Quantitative results

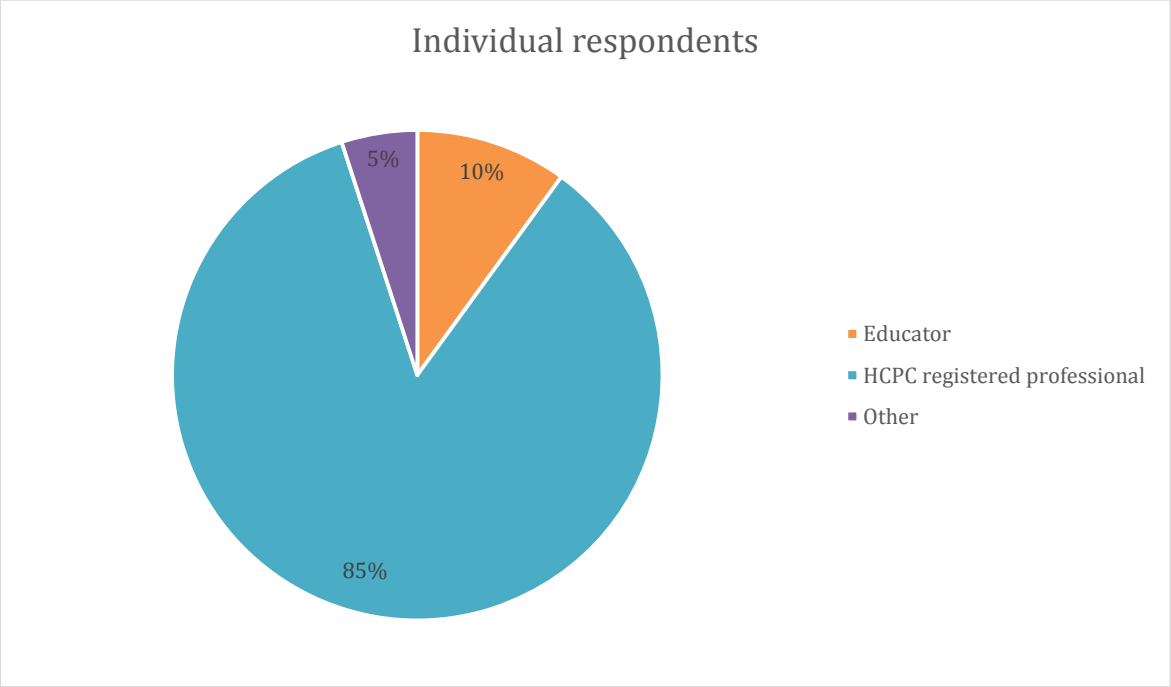
Questions	Yes	No	Partly	Don't know	No answer
Is the revised guidance clear and easy to understand? If not, how could we improve it?	34 (79%)	0 (0%)	6 (14%)	0 (0%)	3 (7%)

Could any parts of the guidance be reworded or removed?	16 (37%)	21 (49%)	2 (5%)	1 (2%)	3 (7%)
Is there any additional guidance needed?	17 (40%)	19 (44%)	0 (0%)	5 (12%)	2 (5%)
Do you have any other comments on the draft guidance?	18 (42%)	23 (53%)	0 (0%)	0 (0%)	2 (5%)

- Percentages in the tables above have been rounded to the nearest whole number and therefore may not add up to 100 per cent.

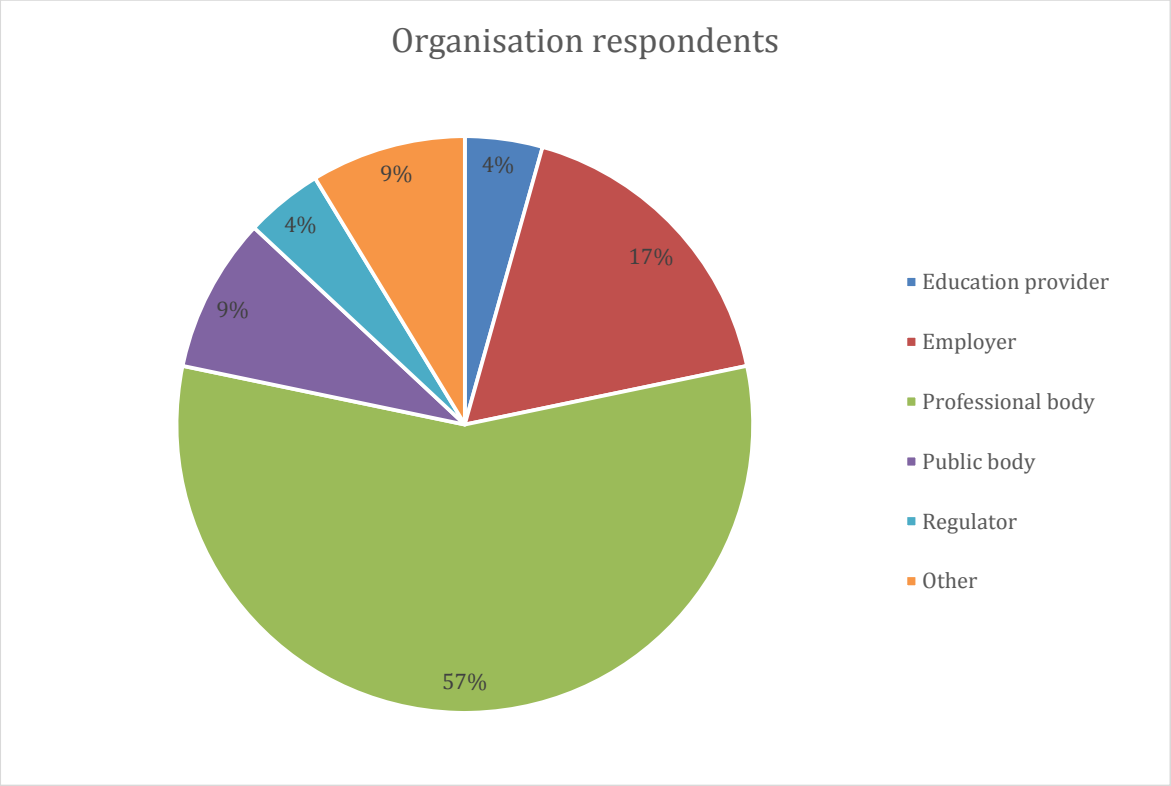
Graph 1 – Breakdown of individual respondents

Respondents were asked to select the category that best described them. The respondent who selected 'other' identified themselves as a joint educator and HCPC registrant.



Graph 2 – Breakdown of organisation respondents

Respondents were asked to select the category that best described their organisation. The organisations who selected 'other' identified themselves as a national association of representatives and a law firm.



3. Summary of responses

3.1 There was strong support from the majority of respondents for the revised guidance on ‘Confidentiality’, although some qualified their response by suggesting further improvements.

3.2 Many respondents welcomed the clear and simple language in the revised guidance.

3.3 A number of comments were made about the differences between consent for confidentiality purposes and consent under the Data Protection Act 1998 (DPA). Respondents stated that further clarification was required in the guidance.

3.4 Respondents also made comments regarding the considerations to be taken ahead of any disclosure of information, requesting further clarification in this area.

3.5 Informed consent and capacity was an area raised by a number of respondents who welcomed further information, particularly in relation to children and young people, and individuals with disabilities. In addition, some respondents requested further guidance on the considerations to be taken when disclosing information without consent.

3.6 Several respondents requested additional information about data protection principles.

3.7 Some respondents felt there should be an explicit reference to safeguarding in the guidance.

3.8 One organisation raised concerns about a perceived lack of information relating to the position in Scotland, and requested further consideration be given to this in the guidance.

4. Responses to the consultation

4.1 There was overall support from respondents for the revised guidance on ‘Confidentiality’, with some comments for further amendments to improve the content and accessibility of the document.

4.2 The comments we received are summarised below, structured around the common themes we have identified.

Language and style

4.3 The majority of respondents (79%) considered that the revised guidance was clear and easy to understand. Of those respondents who provided additional comments, 52% specifically welcomed the changes to the language and style of the document.

4.4 A number of suggestions were made regarding the language and style of the document to improve ease of reading, these included:

- numbering the section headings for ease of reference;
- providing some broad reference to key pieces of legislation, for example, referring to ‘data protection and freedom of information legislation’; and
- replacing the term ‘service user’ with ‘patient’.

Consent and disclosure

4.5 Two organisations raised concern that the differences between consent for confidentiality purposes, and consent under the Data Protection Act 1998 (DPA) weren’t sufficiently covered in the draft guidance. Specifically that, for consent to be valid under the DPA, it must be equivalent to express consent for confidentiality purposes. Furthermore that where an HCPC registrant needs to share information with others who are involved in a service user’s care and treatment under the DPA, this is covered by condition 8 of schedule 3 rather than implied consent.

4.6 One organisation commented that the principle requiring registrants to ‘only disclose identifiable information if it is necessary, and, when it is, only disclose the minimum amount necessary’ is too narrow, as registrants are under an obligation to protect the confidentiality of all service user data.

4.7 Another organisation stated that it would be helpful to clarify that regulators may have statutory powers to request information, and where they don’t, registrants will need to consider whether disclosure is necessary in the public interest.

4.8 One respondent raised concern about the appropriateness of gaining express consent verbally, whilst another asked for clarity in the guidance on how consent should be documented.

Informed consent and capacity

4.9 Several respondents commented that the draft guidance would benefit from more detail around informed consent and capacity, particularly for service users with disabilities. One individual suggested including a simple list of criteria.

4.10 One respondent suggested that it would be helpful for the document to provide further guidance in relation to children and young people, particularly for sole or self-employed practitioners who aren't able to reply on employer policies.

4.11 A number of respondents raised concern about the reference to 'best interest' in the guidance. One individual suggested that the Mental Capacity Act 2005 should be referenced alongside any reference to best interest as an individual reading the guidance could infer that they could make the decision with no discussion or involvement from others. There was concern this could negatively impact those who don't have capacity. One organisation raised concern that best interests is not a relevant consideration, or basis for decision-making on behalf of others for adults in Scotland, and has been explicitly rejected as a relevant test in the *Scottish Law Commission Report on Incapable adults (Report No 151)*.

Disclosing information without consent

4.12 A number of respondents commented on the need for additional guidance in relation to the disclosure of information without consent. One organisation stated that, under the DPA, if the disclosure has a legal basis anyway consent may not be required. Instead, they stated that the service user should be notified that the disclosure will take place and given details about who it would be disclosed to and why.

Data protection

4.13 There were a number of comments from respondents requesting further clarification on the approach they should take to data protection, in particular::

- how to manage shared records – how to decide when information should be locked to one professional and when it should be available to the whole team managing the care;

- how self-employed professionals should approach data protection; and

- how professionals should approach accessing information about themselves and their family and friends.

Safeguarding

4.14 A number of respondents commented on the absence of an explicit reference to safeguarding within the guidance, particularly given the final Caldicott principle which outlines that the 'duty to share information can be as important as the duty to protect patient confidentiality'.

Four country considerations

4.15 One organisation raised concerns about the distinctive and differing Scottish position in relation to consent and disclosure and opined that this should be reflected more thoroughly in the draft guidance.

General comments

4.16 A number of other suggestions were made by respondents about the structure and content of the guidance, including:

- bringing the information about professionals making autonomous decisions about confidentiality and disclosure forward to the front of the document;

- incorporating case studies of different scenarios professionals might face;

- including a reference to the importance of confidentiality in the context of social media.

5. Our comments and decisions

5.1 We have considered carefully all the comments we received to the consultation and have used them to revise the draft guidance. The following explains our decisions in some key areas.

Language and style

5.2 The majority of respondents to the consultation considered that the guidance was clear and easy to understand. However, we did receive some comments on how it could be improved and we have made a number of small changes in response, for example, numbering the section headings for ease of reference.

Consent and disclosure

5.3 Whilst the primary purpose of the guidance is to provide advice on how health and care professionals handle information about service users, in considering the feedback from the consultation it is clear that registrants would benefit from some further high-level guidance in other related areas. With this is mind we have:

- provided additional guidance on issues relating to capacity;
- expanded our guidance on issues relating to children and young people; and
- outlined the factors the Mental Capacity Act 2005 details must be considered when determining best interests.

Data protection

5.4 Some respondents requested further clarification for self-employed professionals around data protection principles, so we have made explicit reference to the need for self-employed professionals to contact the Information Commissioner if they are unsure how to proceed.

Safeguarding

5.5 A number of respondents requested further information on issues relating to safeguarding concerns. In the new guidance we have outlined the need to follow local procedures, or, where there aren't any, we have signposted the appropriate bodies a registrant should refer their concerns to.

Four country considerations

5.6 One organisation raised concerns about the distinctive and differing Scottish position in relation to consent and disclosure. We have, where possible, indicated where registrants in Scotland should take a different approach.

6. List of respondents

Below is a list of all the organisations that responded to the consultation.

Academy for Healthcare Science
Association of Educational Psychologists
Berkshire Healthcare NHS Foundation Trust
BLM (law firm)
British Academy Audiology - Service Quality Committee
British Chiropody & Podiatry Association
British Society of Hearing Aid Audiologists
Canterbury Christ Church University
Centre for Advancement of Interprofessional Education (CAIPE)
College of Occupational Therapists
College of Paramedics
Greater Glasgow and Clyde Health Board - Area Psychology Committee
Information Commissioner's Office
National Community Hearing Association
Northern Ireland Ambulance Service Health and Social Care Trust
Professional Standards Authority for Health and Social Care
Scottish Ambulance Service
The British Dietetic Association
The Law Society of Scotland
The National Association of Educators in Practice (NAEP)
The Society of Chiropodists and Podiatrists
UNISON
Unite the Union