


Contents	2
Introduction	4
What is transparency?	7
How do we develop transparency information?	13
How do we provide transparency and privacy information?	19
How do we assess if we are being transparent?	24
Glossary	26

Contents

We're looking for your thoughts on the impact of this guidance and how we may be able to make improvements. [Click here to complete our impact survey](#) .

Introduction

- [Introduction](#)
- [Who is this guidance for?](#)
- [What is a legal requirement in this guidance and what is good practice?](#)

What is transparency?

- [What is transparency?](#)
- [How does this guidance approach transparency?](#)
- [Why is transparency in health and social care so important?](#)
- [What do we need to do before we consider transparency?](#)
- [When do we do a DPIA?](#)

How do we develop transparency information?

- [How can we demonstrate that we are open and honest?](#)
- [How should we reflect choice?](#)
- [How do we identify harms arising from a lack of transparency?](#)
- [How can we involve the public?](#)

How do we provide transparency and privacy information?

- [How do we provide transparency and privacy information?](#)
- [What are the most effective ways of communicating with your audience?](#)
- [How direct do communication methods need to be?](#)
- [How should we layer our privacy and transparency information?](#)
- [How do we deal with complexity and prevent 'information overload'?](#)
- [How should we work together?](#)

How do we assess if we are being transparent?

- [How do we assess if we are being transparent?](#)
- [How often should we review our transparency information?](#)
- [Transparency checklist](#)

Glossary

- [Glossary](#)

Introduction

In detail

- [Introduction](#)
- [Who is this guidance for?](#)
- [What is a legal requirement in this guidance and what is good practice?](#)

Introduction

Transparency is a key principle of the Data Protection Act 2018 (DPA 2018) and UK GDPR. Transparency ensures that people are aware of how you use their personal information. This means they can then make informed choices about how to exercise their information rights.

Being transparent about how you use personal information also has an important role to play in increasing levels of trust and confidence. A lack of transparency can negatively impact levels of trust and lead to poorer outcomes for patients, service users and the public.

Within health and social care, new technologies that use large amounts of personal information are being developed to support both direct care and secondary purposes, such as planning and research. An example of this is the use of Secure Data Environments (SDE). These are secure environments that provide remote access to anonymised health information, whilst protecting people's privacy. Although these data-driven solutions offer many benefits to the public, you **must** still explain them clearly to people to increase trust and to comply with data protection requirements. This is true of all uses of personal information across health and social care settings. It is important that you are transparent whenever you are using personal information.

We have developed this guidance to help organisations that process health and social care information to understand our expectations about transparency.

Existing guidance

This guidance supplements existing ICO guidance on areas linked to transparency. We would advise you to read this separately in order to have a better understanding of how to comply with legal requirements. We will include links in our 'further reading' boxes where relevant throughout the document on:

- [the principle of transparency](#);
- [the right to be informed](#); and
- [using clear and plain language](#).

We have also provided a [glossary](#) as an annex to help you understand the terms we use in this guidance.

Who is this guidance for?

The audience for this guidance is any organisation (including private and third sector organisations) who delivers health and social care services or processes health and social care information, including for

secondary purposes (such as research and planning). This also includes:

- local government organisations engaging with health and social care services;
- suppliers who are using personal information to support the health and social care system;
- universities using health information for research purposes; and
- other public services that use health information for their own purposes (eg fire service, police and education).

This guidance is also aimed at anyone in health and social care who is involved in preparing and delivering transparency information to the public. This can include:

- policy makers;
- information governance staff;
- data protection officers (DPOs);
- service managers or clinicians with data protection responsibilities (where appropriate in smaller health and social care settings);
- communications and media teams; and
- product teams responsible for explaining new technological solutions.

Although a range of people may be involved in developing and delivering transparency information, remember that it is a data protection requirement. It is important to involve your DPO or someone with the same responsibility in your organisation. Whilst frontline health and social care staff should be able to explain and signpost to transparency information, they are not the intended audience for this guidance.

This guidance will help you to understand:

- what data protection transparency means for health and social care organisations;
- how to develop effective transparency material;
- how to provide transparency and privacy information to people; and
- the factors to consider when assessing your organisation's level of transparency.

Your transparency measures **should** be proportionate to your processing activities and the data protection risks to the public. Whilst this guidance is applicable to all organisations within the health and social care sector, you will need to assess how much it applies to your organisation. For example, a small GP practice making minor updates to their privacy notice would not have to consider the steps outlined in this guidance in as much detail as a hospital trust implementing a new health record system.

Examples of activities where this detailed guidance may be useful include:

- implementing a new data collection to support secondary purposes (ie a new research tool);
- setting up a shared care record across a region to support direct care;
- informing people about a new personal health record app;
- setting up a research programme where researchers can contact people to invite them to participate in research; or
- setting up a new system that shares hospital discharge data with social care providers.

What is a legal requirement in this guidance and what is good practice?

To help you understand the law and good practice as clearly as possible, this guidance says what organisations **must**, **should**, and **could** do to comply with data protection legislation.

Legislative requirements

Must refers to legislative requirements (**the scope of this guidance is limited to the requirements of DPA 2018 and UK GDPR**).

Good practice

Should does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you **must** be able to demonstrate that this approach also complies with the law.

Could refers to an option for example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

What is transparency?

In detail

- [What is transparency?](#)
- [How does this guidance approach transparency?](#)
- [Why is transparency in health and social care so important?](#)
- [What do we need to do before we consider transparency?](#)
- [When do we do a DPIA?](#)

What is transparency?

Transparency in the UK GDPR is the requirement for organisations to tell people about how they are using their personal information. It forms part of the first principle of the UK GDPR, Article 5(1) which requires that personal information shall be:



“a) processed lawfully, fairly and in a transparent manner in relation to the data subject.”

Transparency also applies to the requirement to let people know how you will use their information (the right to be informed). For more information on the right to be informed, see the further reading box below. You **must** be transparent with people in order to comply with the transparency element of Article 5(1). In this guidance we refer to this as “the transparency principle”.

The overall purpose of transparency is to make sure people are:

- aware of and understand when and how organisations are using their personal information and for what purpose; and
- empowered to make decisions about their information rights based on that knowledge.

You may also be required to act transparently under separate legislation, such as Freedom of Information legislation. However, for the purpose of this guidance, we refer to transparency where it is about:

- the use of personal information;
- data protection harms; and
- risks (eg programme risks) that organisations can mitigate through increased levels of data protection transparency.

Example

An organisation wants to deliver a system to patients using pseudonymised data. However, people do not support it because they do not understand it and fear it will make their information less safe. The organisation needs to identify and address the public's concerns and be transparent about the aims of the system. They need to explain why they are using pseudonymised data and the steps they're taking to keep information safe. Doing this may increase trust and confidence in the system.

Further reading – ICO guidance

- [A guide to individual rights](#)
- [First data protection principle](#)
- [Right to be informed](#)

How does this guidance approach transparency?

To help provide you with clarity for legal compliance and best practice, we use the following terminology when referring to separate elements of transparency:

- **Privacy information:** This describes the specific information you **must** provide to people to comply with transparency obligations under the right to be informed. You need to provide this when you receive information directly (from someone) or from a third party (Articles 13 and 14 UK GDPR).
- **Transparency information:** This describes the total range of material you **should** provide to comply with the transparency principle. This also includes additional information that you **could** provide to people to make your transparency material more effective. You still need to be transparent even when you have received information indirectly.

It is important to note that the transparency principle does not include an obligation to make all the information you hold available. There will be types of information that you may not want to disclose, eg confidential commercial information, and this is acceptable.

Below are some examples of the difference between privacy and transparency information:

Privacy information

A hospital trust publishes on their website a list of third-party organisations they share patient information with to support the provision of care services.

This is privacy information. It is specific information that you are required to provide to people as part of the right to be informed.

Transparency information

The hospital trust also creates a policy document which they publish on their website, choosing to make it available to the public. The policy describes how the trust makes decisions when sharing personal information with research organisations.

This is transparency information. It is about sharing personal information, but is not specified as something that you are lawfully obliged to do as part of the right to be informed or include within a privacy notice.

Neither

The hospital trust creates an organisation chart, which shows the pictures and profiles of the executive team.

This information contains the personal information of the executive team and provides further information about the organisation. However, this is not transparency or privacy information as it does not provide information about how they will use people's personal information.

Why is transparency in health and social care so important?

The health and social care sectors routinely handle information about the most detailed aspects of a person's health and personal life. This information is provided in confidence to trusted practitioners to receive health and social care services. Some of this information will be classed as special category, which is sensitive information that needs more protection. For more information on special category information, see the further reading box below.

Data protection legislation recognises the importance of this special category information. You **must** put additional controls in place to protect it. However, acquiring and maintaining public trust and confidence is also important. This ensures people feel comfortable in sharing their information so that practitioners can use it. This relationship of trust also sets expectations about how you will inform people about the use of their personal information. The transparency information which you provide can be equally as important to people as the privacy information in building this trust and confidence.

Ensuring that people understand what is happening to their information is an important factor in maintaining trust and support in health and social care systems. The need to collect and use health and social care information may be obvious to those seeking care, but there are other, less obvious, uses that may require further explanation. For example, organisations might need to share information for

planning health and social care services or medical research purposes.

People's support for you using their information for secondary purposes is likely to depend on how much they understand the proposed use. People might not reasonably expect you to use their information for a purpose outside of their immediate care or treatment. If it is not clear what you will actually do with their personal information in practical terms, and the potential impact, then it is likely they will be reluctant to agree to you sharing their information. However, people may appreciate the benefits of sharing personal information for certain purposes, such as planning and research. It is more likely that people will be supportive if the explanation is clear. Being transparent about the use of personal information for secondary purposes can help inform people's expectations and build trust.

Example

A person attends a hospital for emergency treatment. They will want and expect the hospital to share their personal information for the purposes of that treatment. In these circumstances, it is not a priority for the hospital to provide transparency and privacy information. Instead, the person can find this information in the hospital's privacy notice at a later date.

Providing more effective transparency information can also help you achieve other legitimate objectives linked to the use of health and social care information. These objectives may include:

- helping people to make decisions which may have an impact on the services they choose to use;
- informing 'opt out' preferences (if these are available) when the organisation uses their information for secondary purposes;
- gaining acceptance for innovative uses of information that have a public benefit (eg the use of AI-based health and social care technologies);
- setting the agenda for public discussions to inform people's expectations about how organisations use their healthcare information (eg do we pass on information? What is the impact of third-party commercial organisations accessing information in this way?);
- complying with the principles of the Caldicott Guardians in England, Wales and Scotland and Personal Data Guardians in Northern Ireland; or
- promoting the benefits and outcomes of certain types of processing to the public.

Further reading – ICO guidance

- [Special category information](#)
- [Privacy-enhancing technologies \(PETs\)](#)
- [Guidance on AI and data protection](#)
- [Right to be informed](#)

National Data Guardian guidance

The National Data Guardian has provided guidance to organisations on promoting benefits where

confidential information is processed without consent for purposes beyond individual care. Whilst the guidance only applies to England, it should be of broader interest to health and social care organisations across the UK.

- [National Data Guardian guidance - What do we mean by public benefit?](#) 

What do we need to do before we consider transparency?

It is important that you know exactly what personal information you plan to use and why you want to use it. The clearer your purpose for using information, the easier it will be for you to develop clear and engaging transparency information.

Before developing your privacy and transparency information, you **must** consider the following:

- **Necessity and proportionality** – you **must** have a clear reason for using the information. You **must** explain why you are processing the information, your legal basis and, if relying upon legitimate interests, what those interests are.
- **Data protection by design** – you **must** introduce safeguards to protect the information. Explaining the steps you have taken to protect people’s privacy within your transparency information (eg pseudonymising or anonymising information where possible) will increase the levels of trust people have in the system.

Further reading – ICO guidance

- [A guide to lawful basis](#)
- [A guide to the data protection principles](#)
- [Designing products that protect privacy](#)
- [Data protection by design and default](#)

When do we do a data protection impact assessment (DPIA)?

In certain circumstances, such as when you are using new technologies, your processing is likely to pose a high risk to people’s rights and freedoms. If so, you **must** conduct a DPIA. This is highly likely when you are using people’s health and social care information. A DPIA is also required when using information on a large scale. However, even when it is not required, using this process can bring broader benefits. For example, you can demonstrate your compliance with data protection principles, including transparency. By documenting the risks you have identified and the steps you will take to mitigate them, you are being transparent about your thinking. Publishing your DPIA, where appropriate, may further help to achieve this and also build trust and confidence. For more information on DPIAs, see the further reading box below.

Further reading

- [Data protection impact assessments \(DPIAs\)](#)

How do we develop transparency information?

In detail

- How can we demonstrate that we are open and honest?
- How should we reflect choice?
- How do we identify harms arising from a lack of transparency?
- How can we involve the public?

How can we demonstrate that we are open and honest?

In order to process data transparently, you **must** be open and honest and comply with the right to be informed. Being open and honest means being upfront with people about how and why you will use their personal information. It is also about making information available as early as possible, in easily accessible and understandable formats using clear and plain language. You **should** give people sufficient time to have meaningful engagement or input on how you are using their personal information.

Articles 13 and 14 of the UK GDPR say what people have the right to be informed about. You **must** provide people with a list of specific information about the collection and use of their information. Organisations usually achieve this by using privacy notices. However, the principle of transparency often extends beyond the information that appears in your privacy notice. You **must** only apply [exemptions](#) about the right to be informed in the limited circumstances where this is appropriate.

Data protection legislation does not specify or limit what information to include as part of the transparency principle. However, providing additional transparency information will help explain how and why you use people's information which will help set expectations and create trust. You **should** decide what extra information to provide, how much is necessary and the most effective way to provide it. This assessment depends on the type of personal information you are using, why you are using it and the effect that this may have on people.

This **could** include providing:

- additional information (beyond privacy information) that explains how you make decisions about the use of personal information;
- confirmation of what you will not do with people's information to provide further reassurance;
- clarity on design decisions (ie about system architecture) and the risks posed to people's rights when introducing new technological systems, as well as safeguards applied to mitigate risks;
- alternative forms of transparency information designed to suit different needs, such as using diagrams, infographics, videos, case studies and storytelling;
- information in accessible formats, such as large print or braille for people who are visually impaired or non-digital forms for those who may be digitally excluded (remember to explain the meaning and context of any images using alt-text fields to support readers using assistive technologies);
- public communications which raise awareness about how you use their information (eg advertising on television or at a bus stop);
- accountability information, including organisational policies (eg information governance policies, meeting

minutes or data sharing arrangements);

- information that explains how other laws beyond data protection (eg health and social care legislation or government directions) provide the basis for organisations using information in certain ways;
- data protection impact assessments (DPIAs) for certain types of processing activities or systems;
- lists of information disclosed to researchers and the reasoning behind this;
- provide further information about how and why you have the data, if you have received it indirectly (from a third party) and how you intend to use it;
- transparency information (including relevant updates) prompted by requests you may already be receiving from people;
- improved information access tools for the public to give them greater visibility of the status of their own information (eg patient portals). This **could** include providing people with specific information about how you used their information (ie which research studies used the data);
- information about the risks or harms people may be exposed to and providing clarity on how you have, or are going to, mitigate these risks or harms if things go wrong, eg following a data breach (similar to the duty of candour principles that exist in health and social care across some UK regions); or
- information that challenges or proactively deals with contentious issues, for example when addressing misconceptions relating to third-party access to sensitive health information.

How should we reflect choice?

The first principle of the UK GDPR requires that you **must** use personal information in a lawful, fair and transparent manner. UK GDPR also provides people with other specific rights over their personal information, for example the right to object. It is only fair that people are made aware of these rights, any circumstances in which they do not apply and can exercise them easily whenever they do apply.

This means highlighting and explaining genuine choices available to people about how you use their information and doing this in a clear and timely manner in your transparency information.

There are limited opportunities for people within a public health and social care system to provide meaningful consent, where data is needed to provide care. This is why the consent lawful basis in the UK GDPR is rarely appropriate in the context of health and social care information. For further information on consent, see the further reading box below.

However, you also need to consider and comply with Common Law Duty of Confidentiality which uses concepts of 'implied' and 'explicit' consent. This is separate from data protection law and the type of consent you need depends on your purpose and differs for direct care and secondary purposes. For example, a research organisation may require a person's explicit consent to access their health records if they have agreed to participate in a research study. In these cases, being transparent is particularly important so that people understand why this duty applies.

When producing your transparency and privacy information, it is important to set out the position clearly in respect of choice:





- **Data protection** – you **must** be clear when you are using consent as a lawful basis to process personal information.
- **Data opt-outs** – the opt-out policies used in the health and social care sector in England are not a

function of data protection legislation. However, the principles of fairness and transparency mean that you **should** clearly inform people about how the opt-outs apply (including how to register or update a preference).

Further reading – ICO guidance

- [When is consent appropriate?](#)
- [Individual rights - guidance and resources](#)
- [Exceptions and Exemptions \(right to be informed\)](#)

Non-ICO Confidentiality Guidance

- England - [Consent and confidential patient information](#) 
- Wales - [Confidentiality: Code of Practice for Health and Social Care in Wales](#). 
- Scotland - [Protecting Patients Confidentiality](#) 
- Northern Ireland - [Code of Practice on Protecting the Confidentiality of Service User Information](#) 

How do we identify harms arising from a lack of transparency?

It is important to anticipate potential harms in the context of transparency when planning how to use people's information.

Harm can be difficult to identify and quantify. However, it is clear that when people do not understand how organisations are using their personal information, this can cause anxiety or a loss of trust. This is particularly true given the sensitivities around the use of people's health and social care information.

Categories of harms include:

- physical harm (physical injury or other harms to physical health);
- material harm (harms that are more easily monetised such as financial harm); and
- non-material harm (less tangible harms, such as emotional or mental distress and social disadvantage).

Harms may fall into more than one of these categories. There may also be a harmful impact on wider society as well as to particular people.

Examples of potential harms to people include:

- **Psychological harms** - when people do not understand the intended use of their health and social care information, this can result in fear, anxiety and embarrassment.
- **Loss of control of personal information** - if you do not provide descriptions of how you use information, do not provide it adequately, or provide information that is overly complex or difficult to locate, it can cause confusion. This can deter people from accessing and reviewing how you will use their information. If people do not know what is happening with their information, they lose control of it.
- **Lack of trust in services** - a lack of transparency about how you use personal information might create anxieties that lead to people being reluctant to engage with services. They may stop using them completely or reduce their use. They may also choose not to be fully open and honest with those providing health and social care. These, in turn, may negatively impact the health and social care they

and others receive.

Examples of potential societal harms are:

- **Damage to public health** – if people choose not to share their personal information, this might lead to a general lack of availability of health and social care information. This might negatively impact medical research. Also, if people in a particular demographic group or those with rare medical conditions choose not to share their information for research or planning, this may result in inappropriate medical findings to them and their needs. Both of these may result in harm and adverse health outcomes to certain population groups and to wider society.
- **Failure of programmes with significant public benefit** - where people are aware of a programme for the proposed use of their health and social care information but do not fully understand what will happen to it, this can lead to the spread of false or inaccurate information. By not providing sufficient and clear information there is a risk that the programme will fail, losing the potential benefits and causing societal harm.

To prevent or reduce harms resulting from a lack of transparency, you **should** identify the risks of failing to provide sufficient transparency material when using health and social care information. In particular, you **should** consider the potential harm that your intended use of information may have on the public.

Example

A health and social care organisation asks a person who is suffering from a rare medical condition if they can pass on their information for research and planning purposes. Whilst the person agrees in principle, the organisation does not provide them with any detail on what information they will use, who will have access to it and exactly what the organisation will use it for. As a result, the person decides that they would prefer not to share their information in this way.

This potentially causes them harm as it reduces the information available to plan their treatment. It may also cause a wider societal harm, as it reduces the already limited research information for the rare medical condition.

One way of identifying harms is through the DPIA process. Once you identify and address a risk of processing, you can seek to mitigate this by providing sufficient transparency information.

How can we involve the public?

The channels you use to provide your transparency information can be just as important as the information you wish to provide. This involves considering both the message you want to send and how you will communicate it. Effective engagement on data protection and information rights can help you develop high quality transparency information that successfully addresses people's needs and priorities.

Health and social care organisations often use patient and public involvement and engagement (PPIE) processes and voluntary and community groups. These make sure that people remain at the heart of decisions being made about them. You **should** consider using these groups to develop and evaluate your transparency material.

This engagement can help you:

- understand the profile of your audience;
- understand how best to communicate with them;
- establish how people understand and respond to transparency information;
- provide people with a sufficient level of detail on how you will use their information;
- design engaging communications products for all members of the public through which you can provide transparency and privacy information, in a format they prefer to engage with;
- develop different material for groups that may require additional support to understand how the use of their information may impact them, or how to exercise their information rights (eg the elderly, those at risk of being 'digitally excluded', or anyone receiving information via an intermediary such as someone with parental responsibility or a carer);
- prioritise the order in which you provide your privacy information to people (often referred to as [layering](#)) based on their preferences and concerns, particularly for complex processing activities or multiple workstreams which may generate extensive privacy material; and
- evaluate the effectiveness of your transparency and communications information.

Meaningful consultation with the public throughout the process of designing or updating transparency information will improve your understanding of their needs, concerns and expectations. It will also help to raise awareness and understanding of how and why you intend to use their information and to show that you will do this in a responsible way.

It is important to include a representative and wide cross-section of the public, for example:

- children;
- people from underrepresented groups; and
- those who are unfamiliar or sceptical about the topic.

You **could** also collaborate with charities. This will help to ensure that the information you provide is tailored to suit the needs of all those likely to access it.

PPIE can take many forms, including workshops, surveys and inviting representatives to join project delivery or governance groups. The process usually consists of holding open discussions with groups and listening to, acknowledging and responding to their views and concerns and working through issues together. It is important to hold open discussions and establish what representatives already know and what they would like to learn. PPIE also prompts recognition of different views and allows the opportunity for the exchange of ideas.

The level of engagement will vary and be proportionate to both the message you want to get across, the size of your organisation and the level of resourcing you have available. It won't always be appropriate to work with the public and representative groups. For example, a small care home may find it more effective to 'road test' a privacy notice on a few residents, rather than commit to a widespread consultation.

Using information that you already hold is another way of establishing what will work best. For example, you might review previous incident logs or complaints to establish whether being more transparent in those circumstances might have reduced the chance of or prevented the issue from happening.

Case study

A medical research organisation acts as an intermediary between clinical organisations (such as GP practices) and research organisations. Through their service, they make anonymised data provided by GP practices available to researchers at academic, industry and government organisations to support public health and clinical studies.

As well as providing privacy and transparency information online, the organisation directly engages with the public through an extensive PPIE programme. The main objective is to establish a sustainable, effective and inclusive dialogue between researchers and clinicians, as well as patients and the wider public.

These PPIE activities include the following:

- Representatives of the organisation presenting at GP 'Patient Participation Group' meetings, to raise awareness amongst patients and to answer any questions or concerns they may have about the GP practice sharing their data.
- Annual patient public engagement workshops to discuss various aspects of information use, obtain feedback from the public and respond to queries.
- Representatives attending conferences attended by GPs or patient representative groups.

As a result of their patient and public involvement and engagement work, the research organisation can provide the right level of detail in their transparency information. This accounts for the concerns and priorities of patients and their representative groups.

Further reading – ICO guidance

- [Right to be informed](#)

How do we provide transparency and privacy information?

In detail

- [How do we provide transparency and privacy information?](#)
- [What are the most effective ways of communicating with your audience?](#)
- [How direct do communication methods need to be?](#)
- [How should we layer our privacy and transparency information?](#)
- [How do we deal with complexity and prevent 'information overload'?](#)
- [How should we work together?](#)

How do we provide transparency and privacy information?

Under the UK GDPR, organisations **must**:

- operate transparently (Articles 5(1)(a)); and
- provide specific privacy information to individuals (Articles 13/14).

These separate requirements mean that you need to think about the most effective ways of providing privacy and transparency information to people. The UK GDPR does not specify the most effective ways. You can achieve this in several ways in the health and social care sector.

Providing **privacy information** means more than just publishing a privacy notice on your website. You **should** make efforts to inform people where they can find your privacy information and notify people when you make significant changes. This **could** involve signposting people to your privacy notice on your website or notifying them directly.

Providing **transparency information** means making additional information available to people to demonstrate openness and honesty. This is a prime opportunity for you to clearly explain how you will use people's information and to build trust and confidence.

Remember – if you have received information about someone from a third party, you still need to tell them you have the information and what you intend to do with it (see our detailed guidance below). In these circumstances, you may be more limited in the way you choose to inform people, as you may not be able to provide that information in person.

Further reading

- [Right to be informed detailed guidance](#)

When assessing how to provide transparency and privacy material to people as part of this requirement, you **should** think about the following questions.

What are the most effective ways of communicating with our audience?

When implementing new ways of using personal information or making changes to your existing activities, you **should** decide on the most effective ways of informing people. An effective method is one which increases awareness and understanding in how you are using people's information. This may include publishing information on your website, using in-person contact points with the service you offer or a paper form.

You may also decide to use a mixture of communication methods, depending on the audience you are trying to reach. This is where it is important to understand your audience's needs when accessing and understanding the information you wish to provide (for example, providing information in non-digital forms if it's likely that your audience engages with health and social care services in this way).

Some communications methods typically used to provide transparency information include:

- posters and leaflets;
- letters;
- emails;
- texts;
- social media and other advertising campaigns; and
- website pop-ups and just-in-time notifications.

Whatever method you choose, you **must** make your transparency information easy to find. One way of achieving this is to ensure that staff members in your organisation (particularly those with public-facing roles) can provide people with or direct them to relevant information at the appropriate time.

How direct do our communication methods need to be?

You **should** carefully consider how different communication methods can help you provide different elements of your privacy and transparency message. Some methods can engage large audiences (eg a public advertisement), whereas some engage people on a one-to-one basis (eg a letter or email).

In certain circumstances, you **could** decide to use more direct forms of communication, such as providing information in person or writing directly to affected people. Whilst direct forms of communication may not always be necessary or the most appropriate method, you **must** ensure that you have provided people with sufficient privacy and transparency information.

To help you make decisions about contacting people directly, you **should** consider the following points:

- **The impact** – how much this may potentially affect people, including any identified risks or harms. For example, it would not be appropriate to send a letter directly to someone if you are aware that they do not have the capacity to understand the information you need to provide. This might lead to harmful or ineffective outcomes.
- **Public expectations** – as part of your risk assessment and decision making, you may find it helpful to engage with patient and service user groups to understand their expectations about how you would provide transparency information.

Example

An NHS organisation places a series of adverts at bus stops in an area, informing people that organisations can use their information for medical research. The advert lists some of the benefits the public can expect to see as a result. This is an effective way to raise awareness to a large audience about this use of information. However, this method alone is unlikely to provide enough detail to create a deeper understanding of how that process works or to provide any detailed transparency information.

To achieve this, the organisation decides to supplement this awareness raising activity by providing more detailed information directly to people, using leaflets enclosed in appointment letters.

This results in a more rounded and effective transparency campaign.

How should we present our privacy and transparency information?

People may not always have time to read detailed privacy information. Their levels of engagement with this information are also likely to vary, depending on their circumstances and needs at any given time. While certain people may find a detailed privacy notice useful, many people might find the level of information provided in one place overwhelming or too time consuming.

It can be effective to break the privacy information down and offer a layered approach. The first layer typically consists of a short notice containing key information. This may then allow access to a second layer by expanding each section or including links to more detailed information. This may, in turn, contain links to a third layer that explains more specific issues.

You **should** place the most important information prominently within the initial layers of your communication. This will help people engage with the substance of your message and quickly gain a broad sense of what is happening to their information.

The first layer of communication **should** draw people's attention to the most important elements of your privacy information, including:

- a brief overview of how you use their information and for what purpose;
- highlighting any choices or actions available to people about how you use their information; and
- signposting people to areas where they can find out more detailed information (additional layers).

You **could** effectively support these layers through engaging communications products such as infographics and videos.

How do we deal with complexity and prevent 'information overload'?

Some processing activities involving health and social care information can be complex. For example, when multiple, separate programmes are working together as part of a wider programme or strategy to be delivered locally or nationally, the scale can overwhelm people. Other complex processing can involve lots of technical processes, such as implementing privacy-enhancing technologies to deliver enhanced

safeguards to personal information. These types of programmes can generate significant amounts of privacy information if separate privacy notices are required. You **should** consider how to communicate complex or interlinked processing in a clear and accessible manner.

Simplifying your public messaging about these types of programmes can avoid the risk of overwhelming or confusing people. You may find it more effective to pitch transparency material at a high level to ensure people remain engaged and to achieve greater overall awareness.

An alternative method involves breaking down complex information into smaller 'bite-sized' explanations – for further details, please see this section in our guidance on transparency as part of our Children's code (link below). This guidance is also relevant for other types of processing too.

Remember – to make sure your transparency information is easy to understand, you **should** use clear and plain language. This means using everyday terms that people are familiar with and avoiding using confusing terminology or jargon.

Further reading – ICO guidance

- [How should we write and present the information?](#)
- [Children's code - transparency](#)

How should we work with others?

You are responsible for conveying effective transparency and privacy information about your processing activities. However, where organisations are working together to deliver health and social care services, it is important to develop transparency and privacy material that is also 'joined up' in a way that makes sense to people. To do this, you **should** consider how and when people use health and social care services. Those interactions may provide opportunities to provide people with additional transparency and privacy information.

By identifying these opportunities, you can work together with relevant services to plan and allocate responsibility for delivering transparency and privacy information. This can result in successfully delivering this information at the most effective point to people.

Smaller organisations may also utilise relevant information or templates already produced by others to provide information where appropriate.

These solutions can reduce the burden on smaller organisations who may not have sufficient resources to develop and deliver this information.

Example

An Integrated Care System (ICS) decides to implement a new project which involves processing health and social care information. An ICS is a partnership of organisations in the same area that come together to plan and deliver health and social care services. Each of the individual organisations remain

responsible for ensuring that they provide transparency information.

Through the ICS, the organisations can work together to ensure they are providing the same transparency information to the public so there is consistency across the region, without a duplication of effort.

How do we assess if we are being transparent?

In detail

- [How do we assess if we are being transparent?](#)
- [How often should we review our transparency information?](#)
- [Transparency checklist](#)

How do we assess if we are being transparent?

You **must** assess and determine whether you are acting transparently under data protection law, based on your use of personal information and your transparency measures. After you have read this guidance, ask yourself the following questions when you are considering your level of transparency:

- Have your transparency communications increased the level of awareness and understanding of how you use personal information?
- Have you evaluated this in some way? You **could** use patient engagement processes (PPIE) to help you evaluate your transparency material.
- Have you identified transparency issues and made improvements in response?
- Beyond your privacy notice, what additional transparency material have you provided to people?
- How proactive have you been in providing transparency and privacy information directly to people?

How often should we review our transparency information?

You **should** continue to review and evaluate your transparency and privacy information at regular intervals (or at key milestones) to:

- check that it actually explains what you do with people's personal data; and
- ensure that it remains accurate and up to date.

Transparency checklist

This checklist gives you practical steps to help you achieve compliance:

- Before we started developing our transparency information, we understood how we would use the information, identified a lawful basis and assessed the data protection risks.
- We have involved our DPO or those who are responsible for information governance when developing our transparency material.
- We know what privacy information we **must** provide within our privacy notice.
- We have thought about what [additional information or material](#) we can usefully provide to people to increase transparency.

- We have considered the [potential harms](#) associated with failing to provide adequate levels of transparency information.
- We have employed [public engagement](#) processes to develop and refine our transparency material.
- We have considered and implemented the most [effective means](#) to communicate our transparency information to people.
- We have determined what information is [most important](#) to people to include in the initial layers of our privacy and transparency information.
- We have allocated responsibility for delivering transparency [where it is most effective](#).
- We will continue to review and evaluate our transparency measures regularly (again, using public engagement processes where appropriate).

Glossary

This glossary is a quick reference for key terms and abbreviations used in this guidance. It includes links to further reading and other resources that may give you useful context and more detail.

Please note, this glossary is not a substitute for reading this guidance, the ICO's other guidance and associated legislation.

Anonymised

The UK GDPR refers to 'anonymous information'; information that is not about anyone, and is therefore is no longer 'personal data' and is not subject to the obligations of the UK GDPR.

In order to determine whether data is anonymised, you should consider all the means that a third party may reasonably use to directly or indirectly identify someone. Please check the ICO website for the most recent guidance.

DPA 2018

Data Protection Act 2018. This sits alongside the UK GDPR and sets out the framework for data protection in the UK. See our [guidance about the DPA 2018](#) for more information.

Just-in-time notices

Relevant and focused privacy information delivered at the time you collect individual pieces of information about people.

Layering

A layered approach - short notices containing key privacy information that have additional layers of more detailed information.

Personal information (or personal data)

Defined in UK GDPR Article 4(1) as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

For more information, see our guidance on [what is personal information?](#)

PET

Privacy-enhancing Technologies – A broad range of technologies that are designed for supporting privacy and data protection.

For more information, see our [guidance on privacy-enhancing technologies](#).

PPIE

Patient and public involvement and engagement

Pseudonymised

Data which has undergone pseudonymisation is defined in the UK GDPR as data that can no longer be attributed to a data subject without the use of additional information. You must ensure that the additional information is kept separately, and that appropriate technical and organisational controls are in place to ensure that re-identification of an individual is not possible. Please check the ICO website for the most up to date guidance.

SDE

[Secure Data Environment](#) – A secure data and research analysis platform. Part of the NHS Research SDE Network. It gives approved researchers with approved projects secure access to NHS healthcare data.

Special category data

Defined in UK GDPR as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”.

For more information, see our guidance on [special category data](#).

UK GDPR

The United Kingdom General Data Protection Regulation. This sets out the framework for data protection in the UK along with the DPA 2018.

Using (Processing)

Processing is defined in UK GDPR as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.