**Health and care:**

**Template privacy notice (PN)**

**Background**

Being open with people about how you use their information is a key requirement under the UK General Data Protection Regulation (UK GDPR) and shows people that you care about their information. Explaining to people in advance what you will be doing with their information helps to build trust, avoid confusion, and lets everyone know what to expect.

Organisations that hold personal information, such as people’s names and contact details, must produce a privacy notice. A privacy notice explains why you need people’s personal information, what you plan to do with it, how long you will keep it, and if you will share it with anyone else.

Your privacy notice needs to include details of people’s information rights. It should also tell people how they can complain if they have concerns about the way you are using their information.

People should understand that the information collected is relevant and necessary to the purpose(s) you have stated. For example, collecting and recording information about a patient’s blood test results is relevant and necessary for the purpose of providing care.

You will need to be able to explain these points in writing in a way that’s easy for people to understand. This could include presenting the information in a layered format on your website so that people can easily click through to the areas they are interested in.

A template privacy notice can be found below. We encourage organisations to adopt this template. The template is written so that it is easy to use without needing expertise in data protection. It is often clearer to produce a separate privacy notice for each purpose you are collecting data, for example one to cover individual care, one to cover research and another to cover job applications. It is the responsibility of your organisation to ensure that the privacy notice is completed appropriately.

If you are a sponsor for research or a research site, you will need to prepare a privacy notice about your use of personal data for research. Research sponsors should refer to the Health Research Authority (HRA) transparency templates for sponsors to support you in this case. NHS sites should provide a link to the HRA [transparency template for sites](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/transparency-wording-nhs-organisations/) as embedded in this template.

Text in [square brackets and green highlight] is guidance only and should be removed before publishing.

Text in yellow highlight is sample wording and should be edited according to your local circumstances.

# [Insert your organisation name] privacy notice for [insert specific privacy notice use here, for example, programme name/individual care/employment and staffing]

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services.

You can find more detailed information about how we your information for the following specific purposes here:

* Research - [Find out](https://www.hra.nhs.uk/information-about-patients/) how health researchers use information [If you participate in research also link to your specific privacy notice relating to research. This should comply with [HRA guidance.](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/) The rest of this privacy notice does not apply to research]
* [Add links to other specific privacy notices for example a privacy notice for a specific project]

# Our contact details

Name: [add organisation name]

Address: [add main postal address]

General phone number: [add phone number]

General inquiries email address: [add email address where applicable]

Website: [add website address where applicable]

We are the controller for your information. A controller decides on why and how information is used and shared. [Delete this sentence if you are not the controller and instead fill in the controller’s contact details below.]

# Data Protection Officer contact details [if applicable]

Our Data Protection Officer is [add name] and is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at [provide the preferred contact details for your Data Protection Officer].

# Controller contact details [if applicable]

[If your organisation is not the controller, add contact details for the controller in this section. If you are the controller then you can delete this section as your details will have been provided above.

There may be more than one organisation listed here together with the contact details (joint controllers). For example, this may apply where organisations are using the data for the same purpose, where you share a dataset with another organisation, or where you have designed a new collection with another organisation. You should be clear which organisation is the main point of contact for individuals]

The controller(s) is/are:

Name: [add name of the organisation which is controller(s)]

Address: [add postal address of the controller(s)]

Phone number: [add phone number of the controller(s)]

Email: [add email address of the controller(s)]

Website: [add website address of the controller(s)]

# How do we get information and why do we have it?

The personal information we collect is provided directly from you for one of the following reasons:

[delete or add reasons as relevant]

* you have provided information to seek care – this is used directly for your care, and also to manage the services we provide, to clinically audit our services, investigate complaints, or to be used as evidence as part of an investigation into care
* you have sought funding for continuing health care or personal health budget support
* you have applied for a job with us or work for us
* you have signed up to our newsletter/patient participation group
* you have made a complaint
* [add other reasons you collect personal information]

We also receive personal information about you indirectly from others, in the following scenarios: [add other organisations and the reason for collecting it]:

* from other health and care organisations involved in your care so that we can provide you with care
* from family members or carers to support your care
* [add other scenarios where you collect personal information indirectly]

# What information do we collect?

## Personal information

[Tell people about the type of personal information you collect. Personal information is any information that can be used to identify a living person. For example an individual's email address, telephone number, or NHS number.]

We currently collect and use the following personal information: [delete or add to list as appropriate]

* personal identifiers and contacts (for example, name and contact details)
* photographic identity (photo ID) (for example, photographs of staff for ID badges or our website)
* [add any other types of personal information]

## More sensitive information

[The UK GDPR gives extra protection to more sensitive information known as ‘special category data’. Information concerning health and care falls into this category and needs to be treated with greater care. Data that relates to criminal offences is also considered particularly sensitive.]

We process the following more sensitive data (including special category data): [delete/add as appropriate]

* data concerning physical or mental health (for example, details about your appointments or diagnosis)
* data revealing racial or ethnic origin
* data concerning a person’s sex life
* data concerning a person’s sexual orientation
* genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
* biometric data (where used for identification purposes)
* data revealing political opinions [unlikely to apply]
* data revealing religious or philosophical beliefs
* data revealing trade union membership [unlikely to apply]
* other [please state any other special category data]
* data relating to criminal or suspected criminal offences

# Who do we share information with?

We may share information with the following types of organisations:

* [list organisation types, for example, hospitals, community care teams, care homes]
* third party data processors (such as IT systems suppliers)
* planners of health and care services (such as Integrated Care Boards)
* other [includes any other types such as education]

In some circumstances we are legally obliged to share information. This includes:

* when required by NHS England to develop national IT and data services
* when registering births and deaths
* when reporting some infectious diseases
* when a court orders us to do so
* where a public inquiry requires the information

We will also share information if the public good outweighs your right to confidentiality. This could include:

* where a serious crime has been committed
* where there are serious risks to the public or staff
* to protect children or vulnerable adults

We may also process your information in order to de-identify it, so that it can be used for purposes beyond your individual care whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

# Is information transferred outside the UK? [If applicable]

[Set out whether any data is transferred overseas and if so where and who it is available to, for example…]

Our data is hosted in [add country] but is only available to our staff and technical support staff in the UK and [add country.]

# What is our lawful basis for using information?

## Personal information

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal information is: [choose from the list below and delete the options that do not apply, so that only the lawful basis you are relying upon remains. Where you are relying on different lawful bases for different parts of your data use, for example, one lawful basis for collecting, and another for sharing, you should specify what each lawful basis is for. Only the lawful bases that apply in health and care have been listed].

(a) We have your consent - this must be freely given, specific, informed and unambiguous. [You should not rely on this for individual care, but it is likely to be needed for the use of website cookies].

(b) We have a contractual obligation - between a person and a service, such as a service user and privately funded care home.

(c) We have a legal obligation - the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

(e) We need it to perform a public task - a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities by law. See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care. [This is mostly likely to be relevant for the provision of NHS and social care services regulated by the CQC.]

(f) We have a legitimate interest - for example, a private care provider making attempts to resolve an outstanding debt for one of its service users.

Other - [please state]

## More sensitive data

[For ‘special category data’, such as data concerning health and care, you will need to select a reason for processing it. As a health and care organisation, you are likely to be processing special category data under one of the following lawful bases:

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

But other conditions (such as (b) Employment, social security and social protection and (j) Archiving, research and statistics (with a basis in law) may apply in particular circumstances. Consent is rarely required for special category data in health and care.]

Under UK GDPR, the lawful basis we rely on for using information that is more sensitive (special category): [Delete so only the lawful basis you are relying upon remains. Only the lawful bases that apply in health and care have been listed]]

(b) We need it for employment, social security and social protection reasons (if authorised by law). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

(f) We need for a legal claim or the courts require it.

(g) There is a substantial public interest (with a basis in law). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

(h) To provide and manage health or social care (with a basis in law). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

(i) To manage public health (with a basis in law). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

(j) For Archiving, research and statistics (with a basis in law). See [this list](https://transform.england.nhs.uk/information-governance/the-laws-that-health-and-care-organisations-rely-on-when-using-your-information/) for the most likely laws that apply when using and sharing information in health and care.

## Common law duty of confidentiality [If applicable]

[Add this section if you are using health and care information. You need to satisfy the [common law duty of confidentiality](#_Common_law_duty) when using health and care information.]

In our use of health and care information, we satisfy the common law duty of confidentiality because: [delete as appropriate]

* you have provided us with your consent (we have taken it as implied to provide you with care, or you have given it explicitly for other uses)
* we have support from the Secretary of State for Health and Care following an application to the [Confidentiality Advisory Group (CAG)](https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/#:~:text=The%20Confidentiality%20Advisory%20Group%20(CAG,Health%20for%20non-research%20uses.) who are satisfied that it isn’t possible or practical to seek consent
* we have a legal requirement to collect, share and use the data
* for specific individual cases, we have assessed that the public interest to share the data overrides the public interest served by protecting the duty of confidentiality (for example sharing information with the police to support the detection or prevention of serious crime). This will always be considered on a case by case basis, with careful assessment of whether it is appropriate to share the particular information, balanced against the public interest in maintaining a confidential health service

# How do we store your personal information?

[Tell people how or where you keep their personal information, including where you use third parties to store data on your behalf, and how long you intend to keep it for. Refer to the NHS Records Management Code of Practice, which also applies to adult social care, for guidance on retention periods. Otherwise, you will need to justify the retention period, stating the lawful basis (where applicable) for retaining the information.

You must also explain how you then intend to securely destroy or dispose of the information, archive it, or take any other action, such as anonymise it. You could reference the Records Management Code of Practice, which recommends disposal actions for different types of records. Alternatively, you could reference your organisation’s records management policy.]

Your information is securely stored for the time periods specified in the [Records Management Code of Practice](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/#appendix-ii-retention-schedule). We will then dispose of the information as recommended by the Records Management Code for example we will: [delete as appropriate]

* securely dispose of your information by [explain how you will destroy or delete their information, for example by shredding paper records, or wiping hard drives to legal standards of destruction].
* archive your information at [explain where you will archive their information, for example, a historically significant service’s record may be archived with the local Archive Service, which is run by the Local Authority].
* take another action [explain what else you will do with their information].

# What are your data protection rights?

[Tell people about their data protection rights. Their rights will differ depending on your lawful basis for using their personal information, so once you know this you can select the relevant sections from the text in the template below to include in your privacy notice. The lawful basis page of the [ICO Guide to the UK GDPR](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/) has a useful table that shows the varying rights that apply depending on the lawful basis.]

If you are relying on people’s consent to use their information, then you should also tell people about their right to withdraw consent and how they can do this.]

Under data protection law, you have rights including:

**Your right of access** - You have the right to ask us for copies of your personal information (known as a [subject access request](https://transform.england.nhs.uk/information-governance/guidance/subject-access-requests/)).

**Your right to rectification** - You have the right to ask us to [rectify personal information](https://transform.england.nhs.uk/information-governance/guidance/amending-patient-and-service-user-records/) you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

**Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances.

**Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

**Your right to object to processing** - You have the right to object to the processing of your personal information in certain circumstances.

**Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at [insert email address, phone number and or postal address] if you wish to make a request.

## Automated decision making [If applicable]

[Give details here about the automated decision making that you undertake. Whilst this type of processing may be complex, you should use simple, understandable terms to explain the rationale behind your decisions and how they might affect individuals. Tell people what information you use, why it is relevant and what the likely impact is going to be. For example, an automated staff recruitment process could decide, without human intervention, which applicants are put forward to interview. We are not currently aware of any examples in health and care of special category data being used as part of automated decision making. If you are using special category data as part of automated decision making, contact england.igpolicyteam@nhs.net for advice]

We may use your information to make automated decisions without human involvement, which could have substantial impact on a person, for example in staff recruitment or staff rostering. We may also use profiling, which refers to the use of personal data to predict things such as an individual’s health.

We use the following automated decision making and profiling: [add details if applicable]

## National data opt-out

[Delete from the below list as applicable]

* we are applying the national data opt-out because we are using confidential patient information for planning or research purposes
* we are not applying the national data opt-out because we are not using confidential patient information for planning or research purposes
* we are not applying the national data opt-out because although we are using confidential patient information for planning and research, an agreed [exemption](https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out#understand-if-the-data-you-use-or-disclose-is-in-scope) applies

[Add text about the national data opt-out if it is being applied]

The information collected about you when you use health and care services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

* improving the quality and standards of care provided
* research into the development of new treatments
* preventing illness and diseases
* monitoring safety
* planning services

This may only take place when there is a clear lawful basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential health and care information is only used like this when allowed by law.

Whenever possible data used for research and planning is anonymised, so that you cannot be identified and your confidential information is not accessed.

You have a choice about whether you want your confidential information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters).

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

# How do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at [Insert your organisation’s contact details for data protection queries].

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO’s address is:

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

ICO website: [https://www.ico.org.uk](https://www.ico.org.uk/)

## Date of last review

[Add the date of the last review of this privacy notice and when the next scheduled review is].