


[NHS Digital](#) >  > [Objective E - Using and sharing information appropriately](#) >

**Principle: E2 Upholding the rights of individuals**

Part of [Objective E - Using and sharing information appropriately](#)

## Principle: E2 Upholding the rights of individuals

[← Previous Chapter](#)

[Principle: E1 Transparency](#)

**Current Chapter**

Current chapter – Principle: E2 Upholding the rights of individuals

[View all](#)

**Next Chapter →**

[Principle: E3 Using and sharing information](#)

**Page contents**

---

[E2.a Managing data subject rights under UK GDPR](#)

[E2.b Consent](#)

[E2.c National data opt-out policy](#)

## E2.a Managing data subject rights under UK GDPR

“You appropriately assess and manage information rights requests such as subject access, rectification and objections.”

## Overview

To achieve this contributing outcome, your organisation needs to assure that it supports individuals in exercising their information rights such as subject access, rectification and objections.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the [mapping exercise](#) published by NHS England and the Department of Health and Social Care (DHSC).

## Subject access requests

For practical guidance on responding to subject access requests (SARs), including the procedures you must follow, the necessary timescales, and the situations in which they can be refused, see [guidance on the NHS England Information Governance \(IG\) Portal](#).

It should be noted that organisations are not required to submit freedom of information (FOI) details for the purposes of the DSPT, however this does not negate or diminish required organisation obligations. For more information, see the [ICO's guide to freedom of information](#).

## The right to rectification

NHS England's IG portal contains guidance on [amending patient and service user records](#).

## The right to erasure

The right to erasure is not absolute and [only applies in certain circumstances](#).

However, it should be considered in situations where it becomes relevant. For example, if an individual consents to their patient story being used in promotional materials, and then changes their mind. You would have to remove that specific information from your promotional materials and systems to comply with the right to erasure.

For more information on where the right to erasure applies, see [ICO guidance](#).

## The right to object

Patients and service users have the right to object to the processing of their data. These should be considered on a case-by-case basis, and where it's not upheld, compelling legitimate grounds must be demonstrated by the organisation.

Where data is being processed for direct marketing purposes, the right to object is absolute.

## Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision solely based on automated processing, including profiling, that results in a legal effect on them or significantly affects them in some other way, such as in the way they receive care. UK General Data Protection Regulation (GDPR) defines 'profiling' as any form of automated processing of personal data to evaluate certain personal aspects of an individual, especially to analyse or predict certain things, including health.

An example of where this could happen in some sectors is artificial intelligence (AI). However, given the UK GDPR right for decisions not to be made solely based on automated processing, health and care professionals would be responsible for making final decisions. See the [AI guidance](#) on NHS England's IG Portal for more information.

Similarly, data used for risk stratification purposes are likely to be subject to review for a decision by a human health and care professional, so this is not considered automated decision making.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- privacy and transparency information (such as privacy notices, public communications with patients and employees)
- anonymised logs of SARs
- training needs analysis
- minutes and terms of reference from steering group meetings
- policy, process, procedure or strategy documents (such as data subject rights)

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

**Indicator(s)  
of good  
practice**

A#2

Relevant staff members recognise that individuals can make information rights requests, the different categories of requests, and what action they should take when they receive one.

---

**Term** 'different categories of requests'

---

**Interpretation** These requests would commonly include:

asking for [access to patient records](#) under the [right of access](#)  
asking for information in a patient record [to be amended](#) under  
the [right to rectification](#)  
See the ICO's guide to individual rights for information about the  
different information rights which need to be upheld under UK  
GDPR.

**Indicator(s)** A#3  
**of good practice**

Responsibilities for information rights requests have been delegated to appropriately trained and resourced staff members who can manage them in line with legal requirements.

---

**Term** 'appropriately trained'

---

**Interpretation** You should define the training required for managing information rights requests in your training needs analysis.

## Additional guidance

For additional guidance, see:

[NHS England | Subject access requests](#)

[NHS England | Amending patient and service user records](#)

[Information Commissioner's Office | A guide to individual rights](#)

## Mapping to other cyber frameworks

NHS England and DHSC have produced a [mapping document](#) showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

---

## E2.b Consent

"You have a good understanding of requirements around consent and privacy, including the common law duty of confidentiality, and use these to manage consent."

## Overview

This contributing outcome requires your organisation to have efficient and informed procedures for managing consent.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the [mapping exercise](#) published by NHS England and Department of Health and Social Care (DHSC).

## Consent

You must ensure that your organisation's policies and procedures relating to consent satisfy both the common law and UK GDPR, which cover two definitions of consent in law.

### Consent under common law

In common law, there is a duty of confidentiality which means that when a patient or service user shares information in confidence it can only be disclosed under [specific circumstances](#). One such circumstance is where the patient or service user consents to the sharing.

An individual's [consent may be implied](#) where their health and care information is shared with the individual's health and care team to facilitate the individual's care. This is because the patient would have a reasonable expectation for relevant confidential patient information to be shared with those caring for them. Even in this scenario, steps should be taken to ensure the sharing lines up with the patient's reasonable expectations, and [individuals can object](#) to the sharing of their information if they wish. If a patient objects to the sharing of their information, the consequences of their decision must be clearly explained to them, bearing in mind that in some circumstances, this will mean that they cannot be treated.

Where an individual's health and care information is used or shared in ways they would not reasonably expect, their consent under the common law duty of confidentiality cannot be implied and you need explicit consent or an [alternative common law basis](#). Consent to share their information with third parties, such as solicitors, friends or family members and [unpaid carers](#) must also be sought. NHS England has published specific [guidance on sharing information with the police](#).

Outside of explicit consent, the common law duty of confidentiality may also be satisfied where there is:

- a legal duty to share information

- an overriding public interest
- an overall benefit to a patient who lacks the capacity to consent

The overriding public interest must clearly demonstrate that the public interest benefits override both the individual's rights and the public interest in maintaining confidentiality.

For more information, see NHS England's [guidance on consent and confidential patient information](#).

## Consent under UK GDPR

Under UK GDPR requirements, consent is one of several legal bases for processing personal data. However, consent is not usually the legal basis relied on where health and care personal data is processed for [individual care](#) or [medical research](#).

An example of where you might rely on UK GDPR consent is when you use photography of patient groups on your website. This would be a use of their personal data which falls outside of other Article 6 legal bases, so UK GDPR consent would be required under Article 6. If you were also to include a patient testimonial containing the patient's health information, an Article 9 legal basis would be required for sharing special category data in addition to the Article 6 legal basis.

## Recording consent

An important part of managing consent appropriately is maintaining up-to-date records. These records of consent should be made wherever a legal, regulatory or professional need arises to document an individual's consent or decision not to give consent, whether under common law or [UK GDPR](#).

For common law consent, examples of situations where information should be recorded include, but are not limited to:

- where a patient or service user has expressed that they do not give consent for their information to be shared for direct care
- where your [Caldicott Guardian](#) decides to share information without consent, for example when information needs to be shared in the public interest

In situations relating to common law consent, individuals' consent preferences should be documented to an appropriate level of detail with legitimate justifications for decisions that have been made.

For UK GDPR consent, see the [ICO's practical guidance](#) for legal expectations on creating, managing and maintaining an ongoing consent record under UK GDPR.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- information provided to explain use of confidential information (such as privacy notices, public communications with patients and employees)

- exemplar documents showing how your organisation manages consent
- training needs analysis
- minutes and terms of reference from steering group meetings
- policy, process, procedure or strategy documents (consent for example)

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

<b>Indicator(s) of good practice</b>	<p style="text-align: right;">A#1</p> <p>Relevant staff members understand when they can rely on implied consent, and when they need to ask for or refresh existing explicit consent under the common law duty of confidentiality.</p>
<b>Term</b>	'Relevant staff members'
<b>Interpretation</b>	<p>These should include anyone who has access to confidential patient information. Examples include, but should not be limited to:</p> <p style="padding-left: 40px;">information governance (IG) staff members who are involved in implementing policies and procedures around consent for different uses of patient and service user information</p> <p style="padding-left: 40px;">members of the clinical care team who would be accessing and sharing confidential patient information to carry out their roles, and would therefore need to know about the conditions for implied consent under the common law duty of confidentiality</p>

## Additional guidance

For additional guidance, see:

[NHS England | Consent and confidential patient information](#)  
[Information Commissioner's Office | Consent](#)

## Mapping to other cyber frameworks

NHS England and DHSC have produced a [mapping document](#) showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.



# E2.c National data opt-out policy

“A robust policy and system is in place to ensure opt-outs are correctly applied to the information being used and shared by your organisation.”

## Overview

To meet this contributing outcome, your organisation needs to ensure opt-outs are correctly applied to the information you use and share.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the [mapping exercise](#) published by NHS England and Department of Health and Social Care (DHSC).

## National data opt out

The [national data opt-out](#) was introduced on 25 May 2018, enabling patients to opt out from the use of their confidential patient information for purposes beyond their individual care and treatment - for research and planning.

There are a number of exemptions to the national data opt-out. For example, where people are using anonymous data such as statistics of how many people received a specific treatment, or where use of the confidential patient information is required by law.

You must ensure that you have a mechanism to apply any opt out decisions to relevant datasets. See NHS England's guidance for detailed information on [how to implement the national data opt-out](#).

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- published compliance statements
- privacy and transparency information (such as privacy notices, public communications with patients and employees)
- training needs analysis
- policy, process, procedure or strategy documents (such objections and national data opt out)
- information asset register or equivalent
- record of processing activities (ROPA) or equivalent



This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Additional guidance

For additional guidance, see:

[NHS England | National data opt-out](#)

## Mapping to other cyber frameworks

NHS England and DHSC have produced a [mapping document](#) showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

---

Last edited: 29 August 2024 9:35 am

[← Previous Chapter](#)

[Principle: E1 Transparency](#)

[Next Chapter →](#)

[Principle: E3 Using and sharing information](#)

---

## Chapters

1. [Objective E - Using and sharing information appropriately](#)
2. [Principle: E1 Transparency](#)
3. **[Principle: E2 Upholding the rights of individuals](#)**
4. [Principle: E3 Using and sharing information](#)
5. [Principle: E4 Records management](#)

## Legal

[Privacy and cookies](#)

[Terms and conditions](#)

[Looking after your data](#)

[Freedom of information](#)

[Modern Slavery Act Statement](#)

[Accessibility](#)

[Change cookie settings](#)

[Copyright \(c\) NHS Digital](#)

## Get in touch

[Contact us](#)

[Press office](#)

[Tell us what you think of our website](#)

[RSS feeds](#)

## Follow us on social media



[Twitter](#)



[Facebook](#)



[LinkedIn](#)



[YouTube](#)