


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

Principle: E3 Using and sharing information

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

Principle: E3 Using and sharing information

[← Previous Chapter](#)

[Principle: E2 Upholding the rights of individuals](#)

Current Chapter

Current chapter – Principle: E3 Using and sharing information

[View all](#)

Next Chapter →

[Principle: E4 Records management](#)

Page contents

[E3.a Using and sharing information for direct care](#)

[E3.b Using and sharing information for other purposes](#)

E3.a Using and sharing information for direct care

"You lawfully and appropriately use and share information for direct care."

Overview

This contributing outcome relates to your organisation facilitating the lawful and appropriate using and sharing of information for direct care.

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).

Using and sharing information for direct care

Your organisation has a duty to share information about a patient or service user for direct care purposes unless a specific exception applies. This is set out in the [Health and Social Care Act 2012](#).

Your organisation's policies and procedures for using and sharing information for direct care should reflect that an appropriate legal basis is considered [under both Common Law and UK General Data Protection Regulation \(GDPR\)](#), and also be informed by the [National Data Guardian's Caldicott Principles](#).

Exceptions

Specific exceptions exist where you would not use or share information, including:

- where a service is an anonymous access provider, such as a dedicated human immunodeficiency virus (HIV) and sexually transmitted disease (STI) service, as set out in the [Health and Social Care Act 2012](#)
- where there are specific other legislation which prevent information being shared such as the [Gender Recognition Act 2004](#)

Your organisation must be aware of these legal restrictions on using and sharing information.

Patient or service user objections

Your policies and procedures for using and sharing information for direct care should cover [patient or service user objections](#) as required by the [Health and Social Care Act 2012](#).

Patient records may indicate that a patient or service user does not want a particular piece of information to be shared. These situations must be considered on a case-by-

case basis, involving health and care colleagues and your Caldicott Guardian as appropriate, balancing the information preferences of the individual and the impact on their care. The impact of any decision to withdraw consent must be clearly explained to the individual, bearing in mind that in some circumstances, this will mean they will not be able to be treated.

Arrangements for information sharing for direct care

If you're routinely sharing data with another controller organisation, it's good practice to have arrangements in place such as:

- data sharing agreements (see [NHS England's Data Sharing and Processing Agreement template](#) for more information)
- agreed policies, processes and procedures (information sharing frameworks, data protection impact assessments (DPIAs))

There are different forms your arrangements for information sharing can take. What's important is that you can demonstrate that you have considered:

- the nature of the information being shared
- measures to ensure the sharing adheres to legal and professional requirements
- roles and responsibilities of those involved in the sharing

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:

- minutes and terms of reference from relevant meetings and groups
- documented evidence of information sharing decisions made (disclosure log for example)
- privacy and transparency information (such as privacy notices or public communications with patients and employees)
- training needs analysis
- policy, process, procedure or strategy documents (confidentiality and data protection for example)
- record of processing activities or equivalent
- data sharing agreements
- data protection impact assessments (DPIAs)

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#1

Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it.

Term

'relevant staff'

Interpretation

These should include anyone who has access to confidential patient information. Examples include, but should not be limited to:

information governance (IG) staff members who are involved in implementing policies and procedures around using and sharing information for direct care members of the clinical care team who would access and share information, if needed, for the direct care of patients and service users

Indicator(s) of good practice

A#1

Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it.

Term

'direct care'

Interpretation

For the purposes of the DSPT assessment, 'direct care' should be interpreted as per the definition given in the National Data Guardian's 2013 [Information Governance Review](#).

Indicator(s) of good practice

A#3

Information which is used or shared for direct care is relevant and proportionate.

Term

'relevant and proportionate'

Interpretation

Assessing the relevance and proportionality of information before using or sharing it forms part of your legal obligations under UK GDPR and professional obligations under the [Caldicott Principles](#).

Decisions made in situations where there is a question over relevance or proportionality should be justified and recorded.

**Indicator(s)
of good
practice**

A#5

Your organisation has an appropriate process in place to enable appropriate non-routine ad hoc data sharing for direct care purposes.

Term

'non-routine ad hoc data sharing for direct care purposes'

Interpretation

Most information sharing for direct care will occur within your organisation.

However, you may receive information requests from health or care organisations for direct care who you do not have data sharing agreements in place with, for example organisations situated abroad. These requests should be considered on a case-by-case basis, with controls to ensure that data protection principles and best practices for information sharing are adhered to. See NHS England guidance on [using and sharing information with confidence](#) for more information.

Additional guidance

For additional guidance, see:

[NHS England | Use and share information with confidence](#)

[NHS England | Information sharing in multidisciplinary teams](#)

[NHS England | Sharing information with the voluntary sector](#)

[NHS England | HIV and sexually transmitted infections \(STIs\)](#)

[Information Commissioner's Office | Data sharing: a code of practice](#)

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.

E3.b Using and sharing information for other purposes

"You lawfully and appropriately use and share information for purposes outside of direct care."

Overview

This contributing outcome relates to your organisation facilitating the lawful and appropriate using and sharing of information for other purposes outside of direct care.

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).

Using information for other purposes outside of direct care

When using confidential patient information for purposes other than individual care, such as planning or research, you must have an appropriate UK General Data Protection Regulation (GDPR) legal basis and ensure you have satisfied the common law duty of confidentiality.

You must always consider whether confidential patient information is actually needed for the purpose. If confidential patient information is essential, then explicit consent is normally required for purposes beyond individual care.

If it's not practicable to seek consent for purposes beyond individual care, approval for sharing for medical research or health service planning can be sought from the Health Research Authority or the Secretary of State for Health and Social Care under the [Health Service \(Control of Patient Information\) Regulations 2002](#). This is often known as 'section 251 support'. Section 251 enables the common law duty of confidentiality to be lifted for a period of time, subject to review, so that confidential patient information can be used without breaching the duty of confidentiality. Refer to [HRA guidance](#) for further information.

Sharing information for other purposes outside of direct care

Your organisation should have procedures in place to deal with requests for information from third parties for purposes outside of direct care, such as:

- research
- [law enforcement](#)
- [investigations and inquiries](#)

Your procedures for dealing with these requests should involve an appropriate legal basis being used [under both common law and UK GDPR](#).

Under common law, this may include consideration of:

- whether it's appropriate to seek explicit consent from the data subject
- whether there is a legal duty to disclose
- whether the public interest served by the disclosure outweighs the public interest served by protecting the confidentiality of the individual concerned
- whether support under section 251 is required to set aside the legal obligation of confidentiality

For UK GDPR considerations, see the [ICO's data sharing code of practice](#).

Your procedures should also be informed by [The Caldicott Principles](#).

Documenting decisions and disclosures

Appropriate members of staff such as your Caldicott Guardian and information governance (IG) steering group should be involved in decisions and procedures associated with using and sharing information for secondary purposes.

For any decisions taken, details should be recorded with a clear UK GDPR legal basis and common law basis identified in line with professional guidance.

There is no mandated format for recording disclosures, however your disclosure log should include:

- nature and quantity of information requested
- details of the requester
- nature and quantity of information given
- names and roles of decision makers
- justifications for any decisions taken
- risk assessments carried out

Arrangements for information sharing for other purposes outside of direct care

If you're routinely sharing data with another controller organisation, it's good practice to have arrangements in place such as:

- data sharing agreements (see [NHS England's Data Sharing and Processing Agreement template](#) for more information)
- agreed policies, processes and procedures, such as information sharing frameworks and data protection impact assessments (DPIAs)

There are different forms your arrangements for information sharing can take. What's important is that you can demonstrate that you have considered:

- the nature of the information being shared
- measures to ensure the sharing adheres to legal and professional requirements
- roles and responsibilities of those involved in the sharing

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:

- minutes and terms of reference from relevant meetings and groups
- documented evidence of information sharing decisions made (disclosure log for example)
- privacy and transparency information (such as privacy notices, public communications with patients and employees)
- training needs analysis
- policy, process, procedure or strategy documents (such as confidentiality and data protection)
- data protection impact assessments (DPIAs)

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

PA#1

Relevant staff members understand which of your organisation's information sharing activities fall outside of direct care.

Term

'relevant staff'

Interpretation Requests to share information (whether written or verbal) should be processed by trained or experienced staff.

If you work in a large organisation, there may be a team who is responsible for managing requests. In smaller organisations there should be an individual who is trained to manage requests.

Indicator(s) of good practice

PA#1

Relevant staff members understand which of your organisation's information sharing activities fall outside of direct care.

Term

'direct care'

Interpretation For the purposes of the DSPT assessment, 'direct care' should be interpreted as per the definition given in the National Data Guardian's 2013 Information Governance Review.

Additional guidance

For additional guidance, see:

[NHS England | Use and share information with confidence](#)

[NHS England | Sharing information with the voluntary sector](#)

[NHS England | Sharing information with the police](#)

[NHS England | Access to the health and care records of deceased people](#)

[NHS England | Inquiries, reviews, investigations and court orders in health and social care services](#)

[Information Commissioner's Office | Data sharing: a code of practice](#)

[Information Commissioner's Office | Sharing personal data with law enforcement authorities](#)

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 9:38 am

[← Previous Chapter](#)

[Principle: E2 Upholding the rights of individuals](#)

[Next Chapter →](#)

[Principle: E4 Records management](#)

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](#)