

Data Security and Protection Toolkit 2024-25

CAF aligned DSPT - Objective E – Using and sharing information appropriately

This session is being recorded and will be uploaded to the CAN workspace

NHS England
31 July 2024



Welcome and agenda for today

Housekeeping

- The session is being recorded and is a one-way broadcast, please use the Q&A function to ask any questions
- The slides and recording will be uploaded to the CAN workspace after there will be a link to the recordings for non-CAN members
- The first three webinars have been uploaded to YouTube (unlisted) and can be accessed here:
Webinar 1 Background and overview: <https://www.youtube.com/watch?v=BG6YE1h4W40>
Webinar 2 Objective A - Managing risk: <https://www.youtube.com/watch?v=2aZ6TyEkUgc>
Webinar 3 Objective B - Protecting against cyber attack and data breaches:
<https://youtu.be/IP0Fs1iX1WU>
- If you experience any technical issues, please leave and re-join the call

Agenda for today

1. Overview of Objective E
2. Quiz on 'essential functions'
3. Question and answer session



Webinar content

Session 3 – Objective E – Using and sharing information appropriately

- Overview – what is in the Objective and which teams need to be involved in responding to it?
- Contributing outcomes – Walking through E1 and E2
- Half Time Quiz (‘essential functions’)
- Contributing outcomes – Walking through E3 and E4
- Q&A session

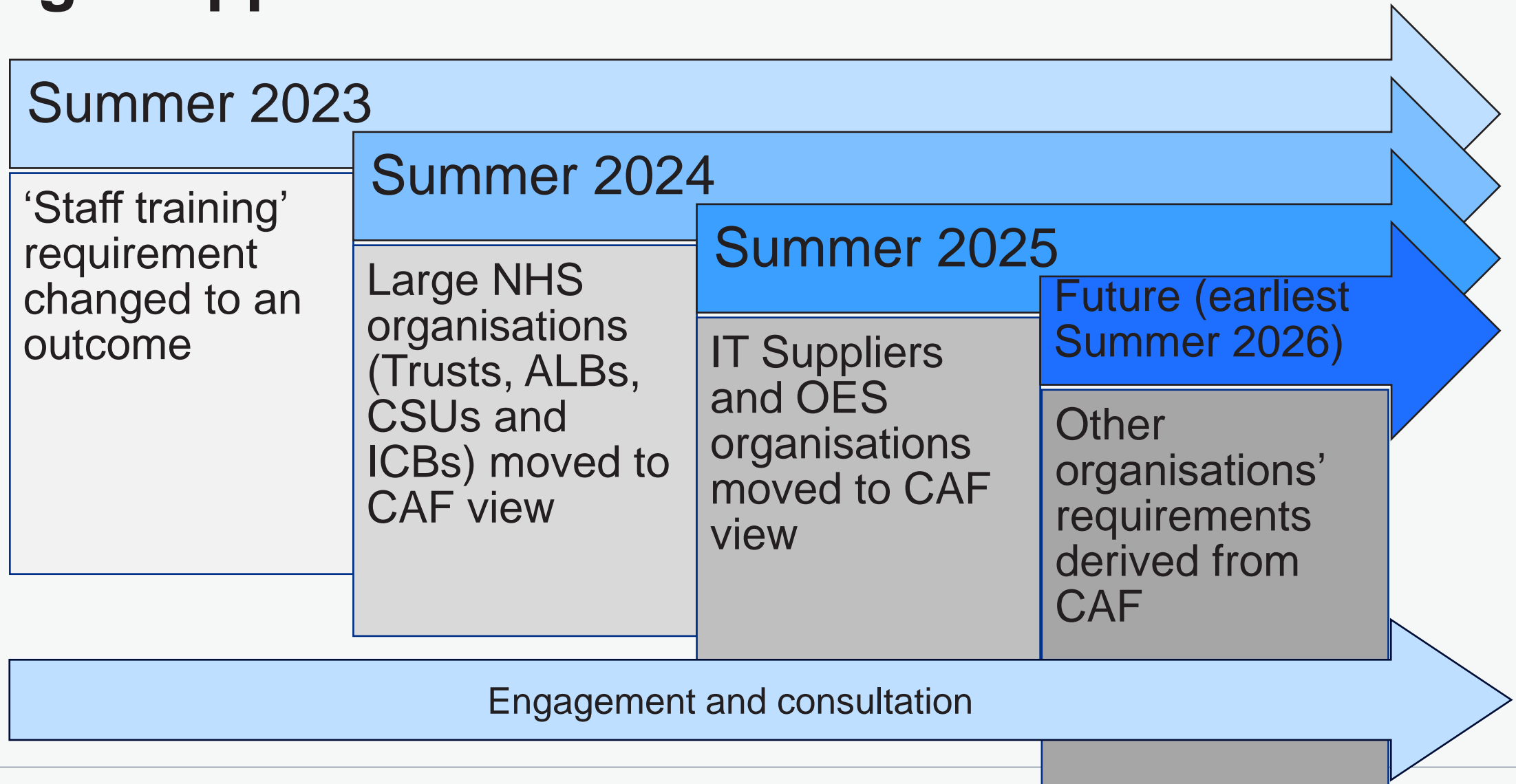
**What is
happening and
why?**


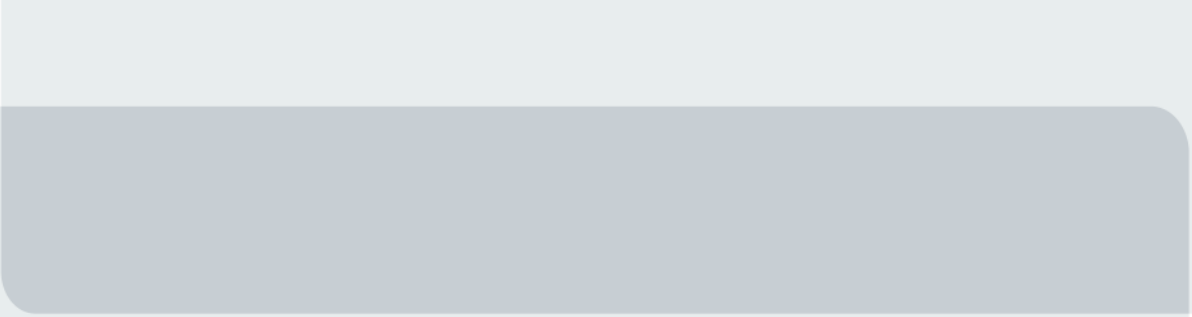


What you need to know

- In September 2024 the DSPT will be changing to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.
- This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes.

Staged approach for DSPT





Objective E - Using and sharing information appropriately

Objective E is **not** “the one IG section”

Objective A – Managing risk

Privacy risk
Data protection impact assessments
Data protection by design & by default
IG roles & responsibilities
Information asset register (IAR)

Objective B – Protecting against cyber attack and data breaches

IG policies & processes
Record of processing activities (ROPA)
Secure storage of data (inc. paper records)
Secure transit of data (inc. paper records)
Training
Culture

Objective D – Minimising the impact of incidents

Responding to data breaches
Notifying impacted individuals
Post-breach controller obligations
Root cause analysis

Objective E – Using and sharing information appropriately

Health and care CAF element		Profile		
Principle	Outcome	NA	PA	A
Objective E - Using and sharing information appropriately				
Transparency	E1.a Privacy and transparency information		PA	
Upholding the rights of individuals	E2.a Managing data subject rights under UK GDPR			A
	E2.b Consent			A
	E2.c National data opt-out policy			A
Using and sharing information	E3.a Using and sharing information for direct care			A
	E3.b Using and sharing information for other purposes			A
Records management	E4.a Managing records			A
	E4.b Clinical coding			A

Principle: E1 Transparency

Contributing outcome: E1.a Privacy and transparency information

You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.

Expectation

The expectation for this contributing outcome is *Partially achieved*

How is your organisation performing against this outcome?

Not achieved
At least one of the following statements is true.

- NA#1 Privacy information is either not available, incomplete, or out of date.
- NA#2 Privacy information is provided in a format that not all patients and service users are able to access.
- NA#3 Privacy information is unclear, overly complex or does not use accessible language.

Partially achieved
All the following statements are true.

- PA#1 Your privacy information is complete and up to date, covering how data is used, what individuals' rights are and how they can exercise them.
- PA#2 Privacy information is easily accessible and provided in a range of different formats for different audiences.
- PA#3 Privacy information is concise, in plain language and communicated in an effective way

Achieved
All the following statements are true.

- A#1 Your privacy information is complete and up to date, covering how data is used, what individuals' rights are and how they can exercise them.
- A#2 Privacy information is easily accessible and provided in a range of different formats for different audiences.
- A#3 Privacy information is concise, in plain language, communicated in an effective way and uses a layered approach.
- A#4 Your organisation publishes relevant data protection impact assessments or summaries of these so that the public can better understand how their data is used and protected.
- A#5 Your organisation effectively uses its communications channels to be transparent about its data use.

Principle: E1 Transparency

Contributing outcome: E1.a Privacy and transparency information

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E1.a Privacy and transparency information: You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.	RAG	1.1.3*

Privacy information

You must provide privacy information about your organisation's data processing activities which informs people about their rights under data protection legislation and how to exercise them. This is a requirement under UK GDPR.

In line with the [Caldicott Principles](#), the information you provide should also ensure there are no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

Individuals must be made aware of this information. It can be sent to them directly via correspondence, or indirectly by leaflets, noticeboards and websites, but it must be easily accessible.

Your organisation must provide information that is:

- concise
- transparent
- intelligible
- clear
- in plain language
- communicated in an effective way

You may choose to display different privacy notices for different audiences. For example, one for staff and another for members of the public. You may also choose to display separate privacy notices for separate processing; one for the use of cookies on your website; another for the data you process for providing care; and a further one for data used for national screening programmes.

For more detailed guidance on transparency information, please see the [ICO's guidance on transparency in health and social care](#). A template privacy notice (PN) produced by NHS England is available on NHS England's [universal information governance \(IG\) templates webpage](#).

Principle: E1 Transparency

Contributing outcome: E1.a Privacy and transparency information

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E1.a Privacy and transparency information: You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.	RAG	() weak ma 1.1.3*

Additional transparency measures

Additionally, where practical, you should provide additional information about your data processing activities to enhance transparency. This means making information such as data protection impact assessments (DPIAs) available to people to demonstrate openness and honesty around specific data processing activities.

To learn more about the difference between privacy and transparency information, see [ICO's guidance on transparency in health and social care](#).

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Privacy information (e.g. privacy notices, public communications with patients and employees)
- Documents supporting scheduled reviews and updates to privacy information
- Transparency information (e.g. published data protection impact assessments (DPIAs), consultations)

This is not an exhaustive list. You are 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.

Principle: E1 Transparency

Contributing outcome: E1.a Privacy and transparency information

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E1.a Privacy and transparency information: You follow best practice for providing privacy and transparency information to ensure that all individuals have a reasonable understanding of their rights and how their information is being used.	RAG	() weak ma 1.1.3*

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 Your privacy information is complete and up to date, covering how data is used, what individuals' rights are and how they can exercise them.	"complete"	To be "complete", your privacy information should <ul style="list-style-type: none"> comply with your transparency obligations under UK GDPR enable patients and service users to have clear expectations about how and why their confidential information is used to satisfy the common law duty of confidentiality <p>NHS England's universal privacy notice template helps you ensure your transparency information covers the necessary information from a health and care perspective.</p>
PA#2 Privacy information is easily accessible and provided in a range of different formats for different audiences.	"range of different formats"	Your privacy information should be available in an appropriate range of formats to ensure that it is easily accessible for your audience. This means considering different: <ul style="list-style-type: none"> publication formats (i.e. web, print) lengths (i.e. concise versions versus more detailed versions)

Additional guidance

For additional guidance, see:

[NHS England | Universal information governance templates and FAQs](#)
[Information Commissioner's Office | Right to be informed](#)
[Information Commissioner's Office | Transparency](#)
[Information Commissioner's Office | Transparency in health and social care](#)

Principle: E2 Upholding the rights of individuals

Contributing outcome: E2.a Managing data subject rights under UK GDPR

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

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Information rights requests under UK GDPR are frequently not recognised or appropriately responded to.
- NA#2 Responsibility for responding to information rights requests has not been assigned to an appropriately trained member, or members, of staff.

Achieved

All the following statements are true.

- A#1 Your organisation appropriately recognises and responds to information rights requests.
- 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.
- A#3 Responsibilities for information rights requests have been delegated to appropriately trained and resourced staff members who can manage them in line with legal requirements.

Principle: E2 Upholding the rights of individuals

Contributing outcome: E2.a Managing data subject rights under UK GDPR

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E2.a Managing data subject rights under UK GDPR: You appropriately assess and manage information rights requests such as subject access , rectification and objections .	R-G	<i>() weak ma</i> 1.2.2* 1.2.3*

Subject access requests

For practical guidance on responding to 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 FOI information 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 is 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.

Principle:
E2 Upholding the rights of individuals

Contributing outcome:
E2.a Managing data subject rights under UK GDPR

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E2.a Managing data subject rights under UK GDPR: You appropriately assess and manage information rights requests such as subject access, rectification and objections	R-G	1.2.2* 1.2.3*

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 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 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) any of the below which best demonstrate your achievement of the contributing outcome:

- Privacy and transparency information (i.e. privacy notices, public communications with patients and employees)
- Anonymised logs of Subject Access Requests (SARs)
- Training needs analysis
- Minutes and terms of reference from steering group meetings
- Policy, process, procedure or strategy documents (e.g. data subject rights)

This is not an exhaustive list. You are 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.

Principle:
E2 Upholding the rights of individuals

Contributing outcome:
E2.a Managing data subject rights under UK GDPR

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E2.a Managing data subject rights under UK GDPR: You appropriately assess and manage information rights requests such as subject access, rectification and objections	R-G	() weak ma 1.2.2* 1.2.3*

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
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.	" different categories of requests "	These requests would commonly include: <ul style="list-style-type: none"> 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 <p>See the ICO's guide to individual rights for information about the different information rights which need to be upheld under UK GDPR.</p>
A#3 Responsibilities for information rights requests have been delegated to appropriately trained and resourced staff members who can manage them in line with legal requirements.	" appropriately trained "	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](#)

Principle: E2 Upholding the rights of individuals

Contributing outcome: 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.

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Relevant staff members are not familiar with the common law duty of confidentiality or privacy rights or do not understand when they need to ask for consent.
- NA#2 You either do not have a policy or procedures in place, or are unsure whether your existing policy or procedures are adequate to ensure that consent is managed appropriately.
- NA#3 Information provided to patients and service users about their consent under the common law duty of confidentiality are either not given or unclear.
- NA#4 You do not have a process for refreshing consent when necessary.

Achieved

All the following statements are true.

- A#1 Relevant staff members understand consent under the common law duty of confidentiality, when they can rely on implied consent, and when they need to ask for or refresh existing explicit consent.
- A#2 Your organisation has a policy and procedures to ensure that consent is managed appropriately, including any decisions made by the Caldicott Guardian.
- A#3 Information provided to patients and service users about the use and sharing of information and consent is appropriate and clear.

Principle: E2 Upholding the rights of individuals

Contributing outcome: E2.b Consent

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
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.	R-G	1.1.3* 1.1.6*

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](#).

Principle: E2 Upholding the rights of individuals

Contributing outcome: E2.b Consent

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
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.	R-G	1.1.3* 1.1.6*

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.

Principle: E2 Upholding the rights of individuals

Contributing outcome: E2.b Consent

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
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.	R-G	1.1.3* 1.1.6*

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Information provided to explain use of confidential information (i.e. 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 (e.g. consent)

This is not an exhaustive list. You are 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.

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 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.	"Relevant staff members"	These should include anyone who has access to confidential patient information. Examples include, but should not be limited to: <ul style="list-style-type: none"> • information governance (IG) staff members who are involved in implementing policies and procedures around consent for different uses of patient and service user information • 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

Additional guidance

For additional guidance, see:

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

Principle: E2 Upholding the rights of individuals

Contributing outcome: 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.

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Relevant staff members are unsure where individuals can opt-out of their data being processed.
- NA#2 You are not sure whether opt-outs have been appropriately applied to relevant data sets.
- NA#3 Your procedure is not robust enough to ensure that all opt-outs are applied and routinely refreshed.
- NA#4 You are unsure whether your organisation is fully compliant with the national data opt-out policy.

Achieved

All the following statements are true.

- A#1 Your organisation understands the circumstances under which opt-outs must be applied and has recorded its applications in the information assets and data flows register.
- A#2 Your organisation clearly communicates to the public where they can opt-out of their data being shared.
- A#3 You have robust procedures and an adequate technical solution in place to ensure opt-outs are correctly applied.

Principle:

E2 Upholding the rights of individuals

Contributing outcome:

E2.c National data opt-out policy

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
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.	R-G	() weak ma 1.2.4*

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 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](#).

Principle:

E2 Upholding the rights of individuals

Contributing outcome:

E2.c National data opt-out policy

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
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.	R-G	() weak ma 1.2.4*

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Published compliance statements
- Privacy and transparency information (i.e. privacy notices, public communications with patients and employees)
- Training needs analysis
- Policy, process, procedure or strategy documents (e.g. objections, national data opt out)
- Information asset register or equivalent
- Record of processing activities (ROPA) or equivalent

This is not an exhaustive list. You are 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.

Additional guidance

For additional guidance, see:

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

Half time quiz

('essential functions')

‘Essential functions’

All assets relevant to the secure operation of **essential function(s)** are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. This includes maintaining an information asset register (IAR) which is reviewed and kept up to date.

You understand the general risks suppliers may pose to your **essential function(s)**.

Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your **essential function(s)**.

Key roles and responsibilities for the security and governance of information, systems and networks supporting your **essential function(s)** have been identified. These are reviewed regularly to ensure they remain fit for purpose.

Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your **essential function(s)** as well as your other data processing activities.

Regular board discussions on the security and governance of information, systems and networks supporting the operation of your **essential function(s)** take place, based on timely and accurate information and informed by expert guidance.

Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the **essential function(s)** as set by senior management.

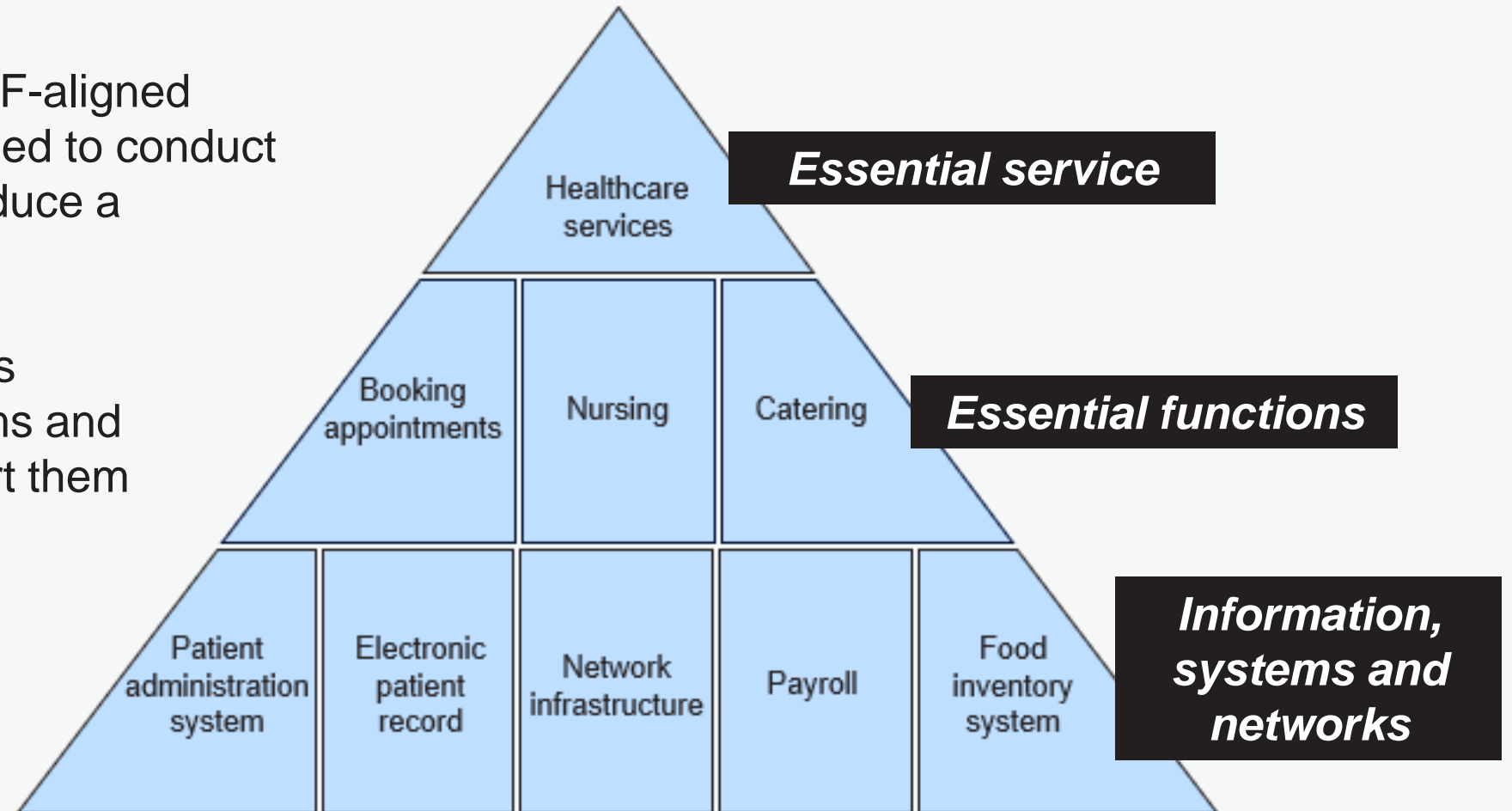
Your organisational process ensures that security and wider Information Governance (IG) risks to information, systems and networks relevant to **essential function(s)** are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process.

You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of **essential function(s)**.

Scoping essential functions

Before you begin your CAF-aligned DSPT submission, you need to conduct a scoping exercise to produce a **document** outlining:

- your essential functions
- the information, systems and networks which support them



'essential functions'

Use your business impact assessments as a starting reference point for the activities which you may want to define as “essential functions”

Activity Reference Number 1		Impact Scoring Key 1 = Negligible - Unlikely to have any impact 2 = Low - May have an impact 3 = Medium - Likely to have an impact 4 = High - Highly probable it will have a significant impact 5 = Very High - Will have a major impact								
Name of Activity: Description of activity: Operational Tasks:		Category of Impacts (please refer to descriptors in the instructions)						Impact Score		
		Length of disruption	Financial	Service delivery	Reputation	Wellbeing, Health & safety	Information security	Statutory / regulatory duty	Business / work plan objective	
		0 - 24 hrs								0.0
		24 hrs. > 7 days								0.0
		7 days +								0.0
		Does the activities vary at different times of the hour, day week, month or year? The above should note the impact at the most important period of activity and will require additional information - enter below								
		If this activity (or similar activity) is also carried out in other Directorates, has a comparison of the RTO, MTPoD and RAG rating been undertaken?								
Recovery Time Objective (RTO)	Maximum Tolerable Period of Disruption (MTPoD)	RAG Rating Score								
		Less than 4.9 is GREEN			Between 5 and 9.9 is AMBER			Over 10 is RED		
		RTO	MTPoD	RPO	RTO	MTPoD	RPO	RTO	MTPoD	
		7 Days+	7 Days+	7 Days+	1 Day	>7 Days	>7 Days	0 Hours	>24 Hours	>2
Activity RAG rating										

> ☰ Front Sheet
🔒 Activity (1)
🔒 Activity (2)
🔒 Activity (3)
🔒 Activity (4)

'information, systems and networks'

Information assets are identified in your information assets & flows registers

Systems (and networks by implication) are identified in your existing inventories of hardware and software assets

Network architecture diagrams show how information, systems, networks fit together

Information Asset Register - an information asset is a collection of information grouped				
Asset number	Asset name	Asset Description	Has a data protection impact assessment (DPIA) been completed for this asset, or the processing this asset relates to?	Which organisation is responsible for the asset (Co
LD001	Staff training files	Certificates and logs of staff training courses, needed to manage and evidence statutory training requirements	No	Dental Pract
NUR002	Shared care records	Shared care records needed to provide individual care	Yes	Health Organis
FIN003	Staff pay data	Payslips and logs relating to staff pay	No	Care Organisa
PAL004	Complaint management records	Record of complaints and descriptions, letters	No	Care Organisa
RD005	Breast cancer research records	Dataset with health details of participants to support research into breast cancer	Yes	Health Organis
FM006	Facilities management contracts	Contracts for all facilities management services for the estate	No	Local Author

‘Essential functions’

All these indicators of good practice are referring to essential functions and information, systems and networks **which you will have documented in your scoping exercise**

All assets relevant to the secure operation of **essential function(s)** are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. This includes maintaining an information asset register (IAR) which is reviewed and kept up to date.

Key roles and responsibilities for the security and governance of information, systems and networks supporting your **essential function(s)** have been identified. These are reviewed regularly to ensure they remain fit for purpose.

Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the **essential function(s)** as set by senior management.

You understand the general risks suppliers may pose to your **essential function(s)**.

Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your **essential function(s)** as well as your other data processing activities.

Your organisational process ensures that security and wider Information Governance (IG) risks to information, systems and networks relevant to **essential function(s)** are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process.

Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your **essential function(s)**.

Regular board discussions on the security and governance of information, systems and networks supporting the operation of your **essential function(s)** take place, based on timely and accurate information and informed by expert guidance.

You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of **essential function(s)**.



Criteria for your DSPT 'essential functions' scope

Does it support the provision of your essential service(s)?

OR

Does it hold personal data?

OR

If compromised by an incident, could it have a cascading impact across your other systems and networks?

If ANY of the above apply, the information / asset / system / network should be included in the scope of your DSPT assessment



Scenario 1

An organisation's electronic patient record (EPR) system.

Would the organisation's EPR be included in the scope of their DSPT assessment?

a) Yes

b) No

Scenario 1

An organisation's electronic patient record (EPR) system.

Answer: Yes.

- EPR **supports** the organisation's provision of healthcare services
- EPR **holds** personal data
- EPR **could have** a cascading impact across other systems and networks if compromised by an incident



Scenario 2

Systems supporting a hospital's retail facilities which:

- **Do not** support the provision of healthcare services
- **Do not** hold any personal data
- **Have been properly segmented** from all other information, systems and networks within the hospital, such that the assessment would be that they have no cascading impact across other systems and networks if compromised

Would the systems supporting these retail facilities be included in the scope of a DSPT assessment?

a) **Yes**

b) **No**

Scenario 2

Systems supporting a hospital's retail facilities which:

- **Do not** support the provision of healthcare services
- **Do not** hold any personal data
- **Have been properly segmented** from all other information, systems and networks within the trust, such that the assessment would be that they have no cascading impact across other systems and networks if compromised

Answer: No.

- These particular systems **do not support** the organisation's provision of healthcare services
- These particular systems **do not hold** personal data
- These particular systems **are assessed to not have** a cascading impact if compromised by an incident



Scenario 3

Children's entertainment systems on a particular ward, which:

Do not support the provision of healthcare services

Do not hold any personal data

Are not properly segmented from all other information, systems and networks within the hospital. There could be a cascading impact across other systems and networks if compromised.

Would these entertainment systems be included in the scope of a DSPT assessment?

a) Yes

b) No

Scenario 3

Children's entertainment systems on a particular ward, which:

Do not support the provision of healthcare services

Do not hold any personal data

Are not properly segmented from all other information, systems and networks within the trust. There could be a cascading impact across other systems and networks if compromised.

Answer: Yes.

- These particular systems **do not support** the organisation's provision of healthcare services
- These particular systems **do not hold** personal data
- These particular systems **could have** a cascading impact if compromised by an incident

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information **for direct care**

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

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Relevant staff members do not understand what direct care is, the activities it covers and when they should use and share information to facilitate it.
- NA#2 Information is not always used or shared when it is needed for direct care.
- NA#3 Information being used or shared for direct care is either inadequate or excessive.
- NA#4 You are unsure whether individuals would reasonably expect their information to be used or shared in all instances where your organisation does so.
- NA#5 There are no arrangements in place for routine information sharing for direct care.
- NA#6 There is no process to share data for non-routine ad hoc direct care purposes, or it is not always followed.

Achieved

All the following statements are true.

- A#1 Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it.
- A#2 Information is used or shared for direct care when it is needed.
- A#3 Information which is used or shared for direct care is relevant and proportionate.
- A#4 When information is used or shared for direct care, individuals' reasonable expectations and right to respect for a private life are considered.
- A#5 Your organisation has a process in place to enable appropriate non-routine ad hoc data sharing for direct care purposes.
- A#6 There are appropriate arrangements in place for information sharing for direct care.

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for direct care

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.a Using and sharing information for direct care: You lawfully and appropriately use and share information for direct care.	R-G	() weak ma (1.1.6*)

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 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 HIV and 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.

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for direct care

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.a Using and sharing information for direct care: You lawfully and appropriately use and share information for direct care.	R-G	() weak ma (1.1.6*)

Arrangements for information sharing for direct care

If you are routinely sharing data with another controller organisation, it is 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 (e.g. information sharing frameworks, data protection impact assessments (DPIAs))

There are different forms your arrangements for information sharing can take. What is 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) any of the below which best demonstrate your achievement of the contributing outcome:

- Minutes and terms of reference from relevant meetings and groups
- Documented evidence of information sharing decisions made (e.g. disclosure log)
- Privacy and transparency information (i.e. privacy notices, public communications with patients and employees)
- Training needs analysis
- Policy, process, procedure or strategy documents (e.g. confidentiality and data protection)
- Record of processing activities or equivalent
- Data sharing agreements
- Data protection impact assessments (DPIAs)

This is not an exhaustive list. You are 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.

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for direct care

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.a Using and sharing information for direct care: You lawfully and appropriately use and share information for direct care.	R-G	() weak ma (1.1.6*)

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
A#1 Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it.	"Relevant staff"	These should include anyone who has access to confidential patient information. Examples include, but should not be limited to: <ul style="list-style-type: none"> 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
A#1 Relevant staff understand what direct care is, the activities it covers, and when they should use or share information to facilitate it.	"direct care"	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 .
A#3 Information which is used or shared for direct care is relevant and proportionate.	"relevant and proportionate"	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.
A#5 Your organisation has an appropriate process in place to enable appropriate non-routine ad hoc data sharing for direct care	"non-routine ad hoc data sharing for direct care purposes"	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](#)

Principle: E3 Using and sharing information

Contributing outcome: E3.b Using and sharing information for other purposes

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

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Relevant staff members are not aware of the circumstances under which information might be used or shared outside of direct care.
- NA#2 Your organisation's practices for using and sharing information for purposes outside of direct care do not satisfy legal requirements including the common law duty of confidentiality, UK GDPR or individuals' right to respect for a private life.
- NA#3 Individuals are not appropriately informed when their information is used or shared for purposes outside of direct care.
- NA#4 There are no arrangements in place for routine information sharing outside of direct care.
- NA#5 You don't maintain an up-to-date disclosure log detailing requests for individuals' information for purposes outside of direct care and sharing decisions your organisation has made.
- NA#6 There is no record of the lawful basis for disclosures that you have made.

Achieved

All the following statements are true.

- A#1 Relevant staff members understand which of your organisation's activities for using and sharing information fall outside of direct care.
- A#2 Your organisation's practices for using and sharing information for purposes outside of direct care satisfy legal requirements including the common law duty of confidentiality, UK GDPR and individuals' right to respect for a private life.
- A#3 Your organisation clearly communicates to individuals where their information may be used or shared for purposes outside of direct care.
- A#4 You maintain a disclosure log which details requests for individuals' information for purposes outside of direct care and sharing decisions your organisation has made, including the lawful basis for the sharing where appropriate.
- A#5 There are appropriate arrangements in place for information sharing outside of direct care.

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for other purposes

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.b Using and sharing information for other purposes: You lawfully and appropriately use and share information for purposes outside of direct care.	R-G	() weak ma (1.1.6*)

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 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 is 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 is 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](#).

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for other purposes

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.b Using and sharing information for other purposes: You lawfully and appropriately use and share information for purposes outside of direct care.	R-G	() weak ma (1.1.6*)

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 are routinely sharing data with another controller organisation, it is 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 (e.g. information sharing frameworks, data protection impact assessments (DPIAs))

There are different forms your arrangements for information sharing can take. What is 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

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for other purposes

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.b Using and sharing information for other purposes: You lawfully and appropriately use and share information for purposes outside of direct care.	R-G	() weak ma (1.1.6*)

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Minutes and terms of reference from relevant meetings and groups
- Documented evidence of information sharing decisions made (e.g. disclosure log)
- Privacy and transparency information (i.e. privacy notices, public communications with patients and employees)
- Training needs analysis
- Policy, process, procedure or strategy documents (e.g. confidentiality and data protection)
- Data protection impact assessments (DPIAs)

This is not an exhaustive list. You are 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.

Principle: E3 Using and sharing information

Contributing outcome: E3.a Using and sharing information for other purposes

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E3.b Using and sharing information for other purposes: You lawfully and appropriately use and share information for purposes outside of direct care.	R-G	() weak ma (1.1.6*)

Interpreting indicators of good practice

Indicator(s) of good practice	Term	Interpretation
PA#1 Relevant staff members understand which of your organisation's information sharing activities fall outside of direct care.	"Relevant staff"	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.
PA#1 Relevant staff members understand which of your organisation's information sharing activities fall outside of direct care.	"direct care"	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](#)

Principle: E4 Records management

Contributing outcome: E4.a Managing records

You manage records in accordance with your organisation's professional responsibilities and the law.

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

- NA#1 Some records are not in the locations indicated on the record keeping system.
- NA#2 You do not have an approved process for disposing of records or it is not routinely followed.
- NA#3 You are keeping data that identifies individuals for longer than it is needed.
- NA#4 Your standards for record keeping are not in alignment with the Records Management Code of Practice.

Achieved

All the following statements are true.

- A#1 Your organisation understands legal and professional obligations for records management.
- A#2 You have a record keeping system implemented at the organisational level which covers every stage of the information lifecycle and arranges records into an appropriate classification scheme.
- A#3 Records are appraised at the end of their retention period and disposed of when appropriate.
- A#4 Data destruction can be evidenced via destruction certificates or equivalent.
- A#5 Your organisation has a robust process to ensure that data that identifies individuals is not kept for longer than necessary.

Principle:

E4 Records management

Contributing outcome:

E4.a Managing records

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E4.a Managing records: You manage records in accordance with your organisation's professional responsibilities and the law.	R-G	1.4.1*

Managing records appropriately

The [Records Management Code of Practice 2021](#) will support you in developing a policy and managing records appropriately. It provides a framework for consistent and effective records management based on established standards. It covers organisations working within, or under contract to the NHS in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities.

Data disposal

Data destruction can be physical (such as shredding) and digital (secure deletion). Your data disposal contracts and suppliers should reference or include guidance on disposal of electronic media containing personal or sensitive data. For further information including on the standards for secure deletion, please refer to the [National Cyber Security Centre guidance](#).

Traditionally, paper-based disposal has consisted of simple vertical shredding. However, this method is not suitable for sensitive or confidential information. [BS EN 15713:2009](#) and the HMG Information Assurance Standard (IS5) requires the shredding of sensitive paper records to be conducted using a [cross cut](#) shredder that cuts the paper into pieces of no more than 15mm x 4mm.

Principle: E4 Records management

Contributing outcome: E4.a Managing records

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E4.a Managing records: You manage records in accordance with your organisation's professional responsibilities and the law.	R-G	1.4.1*

Destruction via third party suppliers

If your organisation uses third parties to dispose of (destroy by any means, including incineration) or archive personal data, there should be a contract in place which requires the third party to have appropriate security measures in place in compliance with data protection law.

Your third-party supplier should record each item that has been disposed of on a destruction certificate. This can be one certificate per item, or multiple items on one certification. It is important that these items are known and can be referenced individually.

A destruction certificate with the following line item is not acceptable given that items have not been referenced individually and they are untraceable:

- 50 x SATA mixed sized hard drive destroyed

Whereas a destruction certificate such as the below, where items are individually referenced and the disposal method is specified, would be acceptable:

- Hitachi (HGST) 500gb 500 GB 2.5 Inch 5400 RPM Sata Hard Drive (s/n 999787989ui9) status shredded
- Western Digital Scorpio Blue 500GB Sata 8MB Cache 2.5 Inch Internal Hard Drive (s/n WD21377878nh98) status shredded

See 'B3.e Media / equipment sanitisation' for more information relating to reuse, repair, disposal or destruction of devices, equipment and removable media.

Principle:

E4 Records management

Contributing outcome:

E4.a Managing records

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E4.a Managing records: You manage records in accordance with your organisation's professional responsibilities and the law.	R-G	1.4.1*

Supporting evidence

To support your response, you can review and upload (or link to) any of the below which best demonstrate your achievement of the contributing outcome:

- Policy, process, procedure or strategy documents (e.g. records management, records classification scheme)
- Minutes and terms of reference from relevant meetings and groups
- Training needs analysis referencing records management requirements
- Spot checks confirming integrity and availability of records
- Data protection impact assessments (DPIAs) conducted in relation to records management
- Certificates of destruction or accession to local place of deposit
- Lists of records which have been disposed of

This is not an exhaustive list. You are 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.

Additional guidance

For additional guidance, see:

[NHS England | Records Management Code of Practice](#)

Principle:
E4 Records management

Contributing outcome:
E4.b Clinical coding

You are committed to regularly evaluating and improving your organisation's coded clinical data.

Expectation

The expectation for this contributing outcome is **Achieved**

How is your organisation performing against this outcome?

Not achieved

At least one of the following statements is true.

NA#1 Your clinical coding practices are not compliant with current national clinical coding standards for the ICD-10 and OPCS-4 classifications.

Achieved

All the following statements are true.

A#1 Your clinical coding practices are compliant with current national clinical coding standards for the ICD-10 and OPCS-4 classifications.

Principle: E4 Records management

Contributing outcome: E4.b Clinical coding

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E4.b Clinical coding: You are committed to regularly evaluating and improving your organisation's coded clinical data.	R-G	<i>() weak ma</i> 1.1.7-8*

Data quality

You should have regard to relevant [information standards](#), data quality sources and related resources to inform your internal policies, processes and procedures for data quality.

This is important to ensure that collection of data is consistent throughout the NHS and other care providers. It also supports the flow and quality of information used, so that health and care professionals are presented with the relevant information where and when it is required to provide effective care and treatment to service users.

See [detailed data quality guidance](#) for more information.

Clinical coding

Organisations depend on clear, accurate coded clinical data to provide a true picture of patient hospital activity and the care given by clinicians.

Coded clinical data is important for:

- monitoring provision of health services across the UK
- research and monitoring of health trends
- NHS financial planning and payment
- clinical governance

See [detailed clinical coding guidance](#) for more information.

Principle:

E4 Records management

Contributing outcome:

E4.b Clinical coding

Mapping, Guidance and Evidence to upload

Contributing outcome	Indicators	DSPT V6
E4.b Clinical coding: You are committed to regularly evaluating and improving your organisation's coded clinical data.	R-G	1.1.7-8*

Training

Training for clinical coding has set standards for:

- the time frame in which it is completed
- the materials used to support it
- who is eligible to undertake national courses

See [detailed clinical coding training guidance](#) for more information.

Audit

There are established procedures in place at acute and mental health trusts for regular quality inspections of the coded clinical data for inpatient and day case episodes. These are undertaken by approved clinical coding auditors using and applying the latest version of the 'Terminology and Classifications Delivery Service' Clinical Coding Audit Methodology to demonstrate compliance with the clinical classifications OPCS-4 and ICD-10.

See [detailed clinical coding guidance](#) for more information.

Principle:

E4 Records management

Contributing outcome:

E4.b Clinical coding

Mapping, Guidance and Evidence to upload

Supporting evidence

The documents which may be appropriate to review and upload in support of your response to this contributing outcome could include:

- Clinical coding audit documentation (e.g. reports, questionnaires)
- Internal audit programme documents
- Minutes and terms of reference from relevant groups and meetings
- Training course registers

Contributing outcome	Indicators	DSPT V6
E4.b Clinical coding: You are committed to regularly evaluating and improving your organisation's coded clinical data.	R-G	1.1.7-8*

Question and answer session

Webinars

Date and time	Topics to be covered
Tuesday 9th July 10:00 – 11:30	Objective A – managing risk
Thursday 18th July 10:00 – 11:30	Objective B – Protecting against cyber attack and data breaches
Wednesday 31st July 10:00 – 11:30	Objective E – Using and sharing information appropriately
Thursday 8th August 14:00 – 15:30	Objective D – Minimising the impact of incidents
Wednesday 14th August 14:00 – 15:30	Objective C – Detecting cyber security events and update on DSPT audits

Please use the link below to register for the webinar series:

[CAF-aligned DSPT 2024-25 webinar series | NHS England Events](#)

You can ask any questions in advance of the webinar using [this form](#).

If you are interested

Thank You



[@nhsengland](https://twitter.com/nhsengland)



[company/nhsengland](https://www.linkedin.com/company/nhsengland)



[england.nhs.uk](https://www.england.nhs.uk)