Part of Objective E - Using and sharing information appropriately

Principle: E4 Records management

← Previous Chapter

Principle: E3 Using and sharing information

Current Chapter

Current chapter – Principle: E4 Records management

View all

Page contents

E4.a Managing records

E4.b Clinical coding

E4.a Managing records

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

Overview

To meet the requirements of this contributing outcome, your organisation must assure that it manages records in accordance with its professional responsibilities and the law. This includes all the types of records which are defined as being covered in the scope of the Records Management Code of Practice 2021.

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).

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.

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's 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.

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:

- policy, process, procedure or strategy documents (such as records management or 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'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 | Records Management 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.

E4.b Clinical coding

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

Overview

This contributing outcome relates to your organisation evaluating and improving its coded clinical data.

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).

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's 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.

Training

Training for clinical coding has set standards for:

- the time frame in which it's 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.

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 (such as reports or questionnaires)
- internal audit programme documents
- minutes and terms of reference from relevant groups and meetings
- training course registers

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 9:39 am

← Previous 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