Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the updated Records Management Code of Practice.

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). He also deals with complaints under the Re-use of Public Sector Information Regulations 2015 ("RPSI") and the INSPIRE Regulations 2009. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

General comments

We welcome this revised Records Management Code of Practice (CoP) for health and social care. As we noted in our previous consultation response[1], there have been a number of developments in the years since the Department of Health released the last CoP. We note that several of these developments have been integrated into the document, including management and destruction of digital records and integrated care records. These are areas where guidance is critically needed in the sector.

We note that this new guidance is much shorter and simpler than the four guidance documents it replaces, which will make it more practical for users. Whilst it is important to keep the CoP brief, there are a few areas where more detail could be provided. For example, while the CoP covers records at contract change in detail, the management of older legacy records is another important issue that is only briefly touched on in this guidance and could be covered in more detail.

Some of the data protection principles are covered more comprehensively than others in the code, and these are generally discussed using different (ie ISO) terminology. Ensuring data is adequate, relevant and not excessive (Principle 3) as well as accurate and up to date (Principle 4) are particular areas of concern that could be covered more comprehensively in the CoP. There have been several incidents and reviews in recent years underlining how inaccurate and incomplete records negatively impact patients[2]. Although there are a few references to reliability and integrity, Principles 3 and 4 could be more explicitly addressed in the CoP.

---

[1] https://ico.org.uk/about-the-ico/consultations/hscic-request-for-feedback-on-revision-of-records-management/

[2] For example, inaccurate and incomplete records were identified as critical gaps in care in a recent review of stillbirths in the UK: https://www.npeu.ox.ac.uk/downloads/files/mbrrace-uk/reports/MBRRACE-UK%20Perinatal%20Report%202015.pdf

Specific comments on Records Management Code of Practice 2015

Types of Records – The first sentence is unclear. Revising this sentence and moving information from the "Social Care and Public Health Records" section (p 13) would provide a more complete explanation of the records covered by the CoP. Under examples, it would be helpful to include an example of a joint social care record.

Introduction – Moving the reference to the DoH Confidentiality Code of Conduct and Security Code from the foreword to paragraph 2 in this section (where confidentiality and security are discussed) would be useful. It is also our understanding that the CQC no longer use Outcome 21 (p 8).

Monitoring – Providing examples of what constitutes evidence of a satisfactory records management regime would help guide users of the CoP. Reference to the DPA principles could be included here, as performance is linked to compliance with the principles.

Legal and professional standards – Regarding the last sentence (p 10), it is unclear how access controls would be implemented in paper records. While retrospective controls are useful for auditing purposes, barrier controls offer more effective protection.

Information lifecycle – The flow diagram (Figure 1) implies that the DPA only applies in the "using" stage, whereas it applies at every stage.

Characteristics of a record – This section focuses on characteristics from the ISO standard. There are also data protection principles from the DPA that are slightly different but must be considered. All principles should be considered in developing a comprehensive records management system, but principles 3, 4, 5 and 7 are especially relevant here and overlap with the ISO characteristics.

DIRKS – An explanation of the purpose of Privacy Impact Assessments, ie to identify and minimise the privacy risks of new projects or policies, would help users know when they might need to conduct one. A link to our CoP[3] could also be inserted here.

Destruction - More detail is needed on putting personal data 'beyond use'. For example, when a legacy system in replaced, the new system should enable permanent deletion. The ICO guidance referenced on p 24 of the CoP includes the caveat that an organisation 'commits to permanent deletion of the information if, or when, this becomes possible'.

The sentence "The ICO has indicated that if information is deleted from the live environment..." (p 24), needs to be clarified. It is correct that our guidance recognises

[3] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

the difficulties faced by organisations with systems where data cannot physically be destroyed and allows for them to comply with the fifth principle by putting it 'beyond use'. However, this CoP does not make clear that our guidance is aimed at those organisations with legacy systems, rather than those seeking to implement new systems. It should be made clear in the CoP that putting information 'beyond use' should be a last resort, rather than a standard option.

Digital records and digital continuity – The document outlines the challenges of retaining a digital record for a long period of time, but it does not address the risks of retaining data for too long. The fifth principle of the DPA requires that personal data be retained no longer than is necessary for the purposes for which it is being processed. The DPA does not set out timescales for retention periods, but data controllers will need to consider the fifth principle along with this CoP in deciding on retention periods.

Digital preservation – As noted in our previous consultation response, any project to digitise records should involve a privacy impact assessment in its early stages to ensure that privacy risks are identified and mitigated where appropriate.

Records at contract change – The issue of managing records at contract change is an important one. The DPA does not prevent sharing records in these circumstances, provided that the processing continues to be fair. The table (p 30) includes some level of fair processing for all scenarios, and it is appropriate that the level of fair processing should differ according to the circumstances. The text could more clearly state, however, that fair processing is required in all circumstances when there is a change in data controllership[4].

The table also indicates that, in some situations, it will not be possible to transfer records because consent cannot be gained. This is a concern given the potentially negative impacts on patient care, and the fact that no information regarding the management of those orphaned records is provided in the CoP. It is important to note that consent is not the only condition in Schedules 2 and 3 under which sensitive personal data can be transferred, and in most cases there will be a condition covering this transfer. The common law duty of confidence is separate from the DPA, but also could accommodate such a transfer for direct care purposes. For example, if the data is being used for secondary purposes, s 251 support should have already been obtained. The data controller could return to the Confidentiality Advisory Group to gain support for this transfer if required.

Family records – This section asks users to take "special care" not to disclose information about an individual to a third party. This is often a risk when responding to a subject access request. The CoP correctly indicates that consent is one way to share

[4] The section on mergers and takeovers in the Data Protection CoP provides more information on the transfer of records: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

third party data. Where consent has not been given (for whatever reason), the data controller is nevertheless required by the subject access provisions to comply with the request and disclose third party information if it is reasonable in all the circumstances to disclose without consent. The ICO's Subject Access Request CoP[5] provides guidance on how to deal with such disclosures.

Integrated records – This is a very important area of records management in health and social care, and this section only briefly touches on such records. As with records at contract change, fair processing notices are critical. Links to more comprehensive guidance on how to insure the governance of such records complies with the DPA is available in the ICO's data sharing CoP[6] and checklist[7].

Social media and bring your own device – The use of mobile technologies and electronic communications present risks to the security of patient data and can lead to accidental disclosures. The CoP rightly points out that texts and emails sent on personal devices should be captured, which is important for ensuring patient records are accurate and up to date (ie Principle 4).

However, the CoP could better address Principle 7, which requires appropriate technical and organisational security measures be in place to prevent incidents such as unauthorised or unlawful processing, or accidental loss of, damage to or destruction of personal data. While the CoP acknowledges the risks to security when an employee leaves the organisation, it should also prompt data controllers to consider when the use of personal email accounts and devices is and is not appropriate. The ICO Bring Your Own Device guidance can help here[8]. We note that the IGA has also recently released brief guidance on the use of mobile devices and bring your own devices; however, it is not clear why this is not linked to or included in the CoP.

An issue not addressed in the CoP is the widespread use of apps to share patient data, and how apps should be treated by records management organisations. Again, the CoP should prompt users of the document to consider not just how the data can be captured in a records system, but whether the use of such apps is appropriate given potential security risks.

Cloud based records – While a link to our guidance is included, this section only mentions the potential to breach Principle 5. There are other risks (eg security) and DPA requirements (eg a written contract) that could be included here.

---

[5] https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
[6] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf
[7] https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf
[8] https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Retention schedule – We welcome the revision of this schedule, as the previous CoP had advised NHS organisations to retain electronic records indefinitely. While the CoP notes that the retention periods in the schedule are minimum periods, it should be noted that this must be balanced against the risk of retaining records for longer than is necessary. The first sentence on p 45 is unclear. Does this refer to the "potential [*to retain*] whole care records"?

We suggest referring back to the appraisal process after the sentence, "The retention periods listed in this retention schedule must always be considered minimum". Otherwise, there is a risk that organisations will take this at face value and retain information for far longer than necessary, risking a breach of Principle 5.

Regarding s 33, this is an exemption for research purposes only, and data controllers will need to determine whether it applies to records on a case-by-case basis. It is also worth noting that this is a limited exemption that applies to some aspects of subject access requests and Principles 2 and 4.

December 2015