NHS
Counter Fraud Authority

Information Sharing Agreements (ISAs)

September 2018

Version 2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
V 1.0	Trevor Duplessis	January 2018	Review June 2018
V 2.0	Trevor Duplessis	September 2018	Update

Table of contents

1. Introduction

1.1 Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure the effective co-ordination and integration of services.

1.2 The Government has also emphasised the importance of security and confidentiality in relation to personal information, strengthening legislation and guidance in this area, building upon the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

1.3 It is important that the NHS Counter Fraud Authority (NHSCFA) protects and safeguards person-identifiable information that it gathers, creates, processes or discloses, so that it complies with the law and any other mandatory requirements applicable to NHS organisations and in doing so provide assurance to the public and stakeholders.

1.4 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual or professional regulatory responsibilities, but is also a requirement within the common law duty of confidence and the data protection legislation.

1.5 This policy sets out the requirements placed on all NHSCFA staff when sharing personal information amongst NHS organisations or between other bodies.

1.6 The Information Commissioner's Data Sharing Code of Practice states that:

'under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors - both public and private. But citizens and consumers' rights under the Data Protection Act must be respected.

Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness'.

1.7 The Caldicott Review "To share or not to share" states that 'The duty to share information can be as important as the duty to protect patient confidentiality'. Those who work in a health and social care environment should, where appropriate, have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles. They should be supported by the policies of their employer, regulator and professional bodies.

1.8 Information can relate to patients, staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held electronically (laptops, palmtops, mobile phones, digital cameras), on paper, storage media (CD/DVD, memory sticks), or even by word of mouth.

2. What constitutes person-identifiable information?

2.1 Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, date of birth, NHS number, post code etc. either directly or indirectly. Such information should not be stored on removable or mobile media unless it is appropriately encrypted and approved by Information Security System team and/or advice sought from the Information Governance Team.

3. What constitutes confidential information?

3.1 Confidential information within the NHS is often commonly thought of as health information; however, it can also include any information that is private and not publicly known information that an individual would expect not to be shared.

4. Scope

4.1 All staff working in or on behalf of the NHSCFA fall within the scope of this policy, including all permanent employees, contractors, interns, temporary staff and those working for NHSCFA on secondment.

5. Purpose of this policy

5.1 The purpose of this policy is to provide a framework for NHSCFA and those working on its behalf to:

- consider the controls needed for information sharing,
- ensure expected standards are met
- establish a mechanism for the exchange of information between NHSCFA and the participating organisation in question.

6. Information Sharing

6.1 Information sharing in the context of this policy relates to the disclosure of personal information between NHSCFA and the other participating organisation(s). Information sharing may take the form of:

- a reciprocal exchange of data
- organisations pooling information and making it available to one another
- organisations pooling information and making it available to a third party
- exceptional, one-off disclosures of data in an unexpected or emergency situation.

6.2 **Sharing non-personal information with other organisations** - Key information may be shared with another organisation to: facilitate the commissioning of services; manage and plan future services; assure and improve the quality of care and treatment; comply with statutory obligations & requests; and/or to audit performance.

6.2. **Sharing personal information with other organisations** - Where necessary and proportionate, personal information may be shared with other organisations to: investigate complaints or pursue/defend potential legal claims; the prevention, detection and investigation of offences; protect vulnerable persons at risk or to assess the probity of service delivery and treatment.

6.3 This policy covers two main types of information sharing:

- 'systematic', routine information sharing where the same or similar data sets are shared between the same organisations for an established purpose; and
- 'ad hoc/ one-off', time restricted, one-off decisions to share information for any range of purposes.

6.4 Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to one-off decisions to share.

6.5 'Systematic' information sharing - This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes and will be governed by established rules and procedures.

6.6 'Ad hoc/ one-off' information sharing - The majority if not most information sharing, takes place in a documented, pre-planned and routine way (as above). However,

there may be occasions when business units/staff may be asked or decide to share information in situations which are not covered by any formal agreement. All ad-hoc or one-off sharing decisions must be carefully considered and documented.

6.7 When deciding whether to enter into an arrangement to share personal data (either as a provider, recipient or both), it is important to consider what the sharing is intended to achieve. Having clear objectives will help identify the following:

- **Could the objective be achieved without sharing the data or by anonymising it?** If so, it would not be appropriate to use personal data where the objective could be achieved using non-personal information.

- **What information needs to be shared?** If the objective cannot be achieved without the sharing of personal data, then only the minimum required to achieve the objective will be shared (see the third Caldicott Principle).

- **Who requires access to the shared personal data?** Only those individuals requiring access to the data to do their job should have access.

- **When should it be shared?** All sharing of data should be accurately documented within a defined set of agreed parameters.

- **How should it be shared?** There should be an agreed process for the secure transmission, receipt, access and retention of the data.

- **How do you check the sharing is achieving its objectives?** Evaluate whether sharing is still appropriate and confirm any safeguards that are in place still match the corresponding risks.

- **How are individuals made aware of the information sharing?** Consider what information is provided to individuals concerned. Where applicable (subject to any relevant exemptions) this needs to be made clear in privacy notices.

- **Are there any risk(s) to the individual and/or the organisation through sharing the data?** Is any individual likely to be damaged by it and where applicable, are they likely to object? Could it undermine the individual's trust in the organisations that hold records about them?

6.8 It is good practice to document all decisions and reasoning related to the information sharing. If there is any doubt about whether it is appropriate to share information advice should be sought from the Information Governance team.

6.9 In all instances where there is a requirement to share information staff must ensure that:

- sharing complies with the law, available guidance and best practice

- only the minimum information necessary for the purpose will be shared

- individual rights will be respected, particularly in relation to confidentiality and security of their information
- confidentiality must be respected unless there is an overriding public interest or a legal justification for disclosure
- periodic reviews of information sharing agreements must be undertaken to ensure that it meets the required objectives/purpose and is still fulfilling its aims.

7. Information Sharing Agreements

7.1 Information sharing agreements set out a common set of rules to be adopted by the organisations involved to facilitate the sharing of information. As part of best practice, all NHSCFA data sharing agreements will be regularly reviewed particularly where information is to be shared on a large scale, or on a regular basis.

7.2 An information sharing agreement should as a minimum, document the following:

- the purpose or purposes, of the sharing
- the data to be shared
- the legal basis for sharing
- the potential recipients and the circumstances in which they will have access
- who the data controller(s) is, any data processor(s) and the data to be shared
- data quality - accuracy, relevance, usability
- data security
- the retention of shared data
- individual rights - procedure for dealing with access requests, queries or complaints;
- review effectiveness/termination of the sharing agreement and any particular obligations on the parties to the agreement, giving an assurance around the standards expected
- awareness of sanctions for failure to comply with the agreement or breaches by individual staff.

7.2 The Information Governance Toolkit[1] (mandatory for NHS organisations) - requirement 14-207, specifies: 'when confidential personal information that can identify an individual is shared, both the disclosing and receiving organisations should have procedures that meet the requirements of law and guidance and make clear to staff the appropriate working practices. In some circumstances these procedures (and the law and guidance on which they are based) should be set out within an agreed information sharing agreement or protocol."

7.3 Where it is decided that a formal Information Sharing Agreement is required between the NHSCFA and a participating organisation, a template agreement can be obtained from the Information Governance Team, following the process outline below.

8. The process

8.1 The business unit will establish where an information sharing agreement is required and provide all of the relevant contact details to the Information Governance (IG) Team.

8.2 Requests for the disclosure of information received from a regulatory body under their regulatory or statutory powers do not fall within the scope of this policy.

8.3 The IG team will provide a template agreement to the business unit, to establish the purpose of the agreement, the data to be shared with the third party/parties and its scope; completing the relevant section(s) of the template and return it to the IG team.

8.4 The IG team will circulate the completed draft NHSCFA internal stakeholders and the Leadership Team for contribution to the agreement, where appropriate.

8.5 The IG team will then establish dialogue with the third party contact to agree and finalise the propose agreement.

8.6 Dialogue is maintained with the third party to agree a final draft, which is circulated to the Leadership Team for comment.

8.7 The final draft is sent to the Senior Management Team for authorisation.

[1] This has now been replaced by the 'Data Security and Protection Toolkit'. This toolkit and its predecessor is a performance tool produced by the Department of Health and Social Care (DHSC). It draws together the legal rules and central guidance relating to information governance and presents them in one place as a set of information governance requirements. Organisations are required to carry out self-assessments of their compliance against the IG requirements.

8.8 Once authorised, the Information Sharing Agreement is published where appropriate to do so.

9. Data Protection Impact Assessment (DPIA)

9.1 Before entering into any data sharing arrangement a DPIA should be undertaken. This will help to assess the benefits that the information sharing might bring to the participating organisations and/or more widely to individuals or society. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy or the likelihood of damage, distress or embarrassment being caused to data subjects.

9.2 As well as any potential harm to individuals, staff should consider the potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared appropriately.

9.3 Any new information assets or data flows that arise out of a new project or procurement where NHSCFA is the data controller or receives personal, confidential, sensitive or business sensitive information will need to be recorded as part of the NHSCFA's wider Information Asset Register.

Further information on DPIAs can be obtained from the IG team.

10. Further advice

10.1 With information sharing there will always be exceptional and difficult circumstances where advice may be needed. The organisation's Information Governance Lead and/or Caldicott Guardians should be consulted where there are any concerns about whether the proposed information sharing is appropriate.

10.2 You should contact the IG team about any exceptional needs or requests for information sharing or decisions that may require input from the Caldicott Guardians.

11. Distribution

11.1 This document will be made available to all staff via NHSCFA's Go2 intranet site.

12. Monitoring

12.1 Compliance with this policy and the process outlined in this document will be monitored via the Finance and Corporate Governance Unit. The Information Governance Lead will be responsible for the annual review and updating of this document.