wellcome trust

SHIP
Scottish Health Informatics Programme

SHIP Guiding Principles and Best Practices

A document of the SHIP Information Governance Working Group

The objectives of this document

This document is a statement of agreed guiding principles for governance and instances of best practice arising from discussions and deliberations of the Information Governance Working Group of the SHIP project. It is intended as a high-level instrument to guide the design and implementation of SHIP while also providing evidence to the public and stakeholders about how SHIP is governed.

This is a living instrument that will be developed and amended as necessary. Key sources of inspiration include the OECD Guidelines on Human Biobanks and Genetic Research Databases (which adopts the Principles and Best Practice approach), various existing Memoranda of Understanding on data sharing and linkage (MoUs) which embody instances of best practice, and research done to date as part of the SHIP project and contained in the Information Governance Scoping Paper (see further the SHIP website).

This document is designed to serve as a good governance template. It is intended as a guide for colleagues involved in SHIP and for others involved in data sharing and information governance both within and beyond the health sectors. It is not intended to cover exhaustively all aspects of governance, nor is it a statement of legal rules. It is assumed that all parties involved in data sharing and linking in the SHIP project are aware of their legal responsibilities and comply with them. This document serves to set the standards according to which SHIP will be governed and against which users will be held. It is an expression of commitment to promote the public interest in scientifically sound, ethically robust research while appropriately protecting the privacy and other interests of the people whose data are used in such research.

The approach of this document follows that of the OECD Guidelines (above) in that it identifies areas of governance which are not found in law or which require further expression and explanation as instances of good governance. As such, it contains a statement of the principles that should guide data sharing and linkage practice as well as instances of best practices drawn from the experiences of colleagues working in SHIP [and which take account of the evidence of public and stakeholder engagement undertaken as part of the SHIP project].

For the purposes of this document:

'Principles' are fundamental starting-points to guide deliberation and action. They reflect the values that underpin the SHIP project and its commitment both to promote the public interest and to protect individual interests. Principles are not rules. Principles sometimes conflict. This is why they are *starting points* for deliberation or action. Because of their fundamental importance, however, it is expected that they are followed where they are relevant to a given data use, storage, sharing or linkage practice. Any departure must be fully and appropriately justified.

'Best Practices' are examples of principles in action. These are instances of optimal governance and in that sense they are aspirational. As with principles, where instances of best practice are not or cannot be followed, clear justification should be offered.

SHIP Guiding Principles and Best Practices

Together, these principles and best practices are an indication of the standards expected within and upheld by SHIP.

A statement about the objectives of SHIP

SHIP is concerned with the appropriate sharing and use of health data for research purposes. Where data are 'personal data' (i.e., relating to an identifiable individual) they enjoy the full protection of the law. This does not means that such data cannot be used for research purposes but strict requirements apply, for example, the consent of the person should be obtained or another justification should be offered, such as the promotion of a significant public interest. Most research does not require personal data and can proceed with 'anonymised data', ie data from which it is not likely reasonably that an individual will be identified. Consent to use anonymised data is not required. However, sometimes research cannot rely on anonymised data and risks to privacy can arise, but consent is not possible or practicable. It is the objective of SHIP to steer a course through these waters.

The two key principles at stake are (1) promotion of the public interest and (2) protection of the privacy and other interests of citizens. Where these coincide, for example when using anonymised data, then the principles align. Where, however, this cannot happen, tensions between the principles can arise. This document provides guidance on reducing this tension, minimising risks and promoting the public interest.

Who is responsible?

"Data controllers" are primarily responsible for overseeing data protection and this instrument discusses their responsibilities (see further Appendix 1). These individuals/organisations, and other responsible parties such as Caldicott Guardians (see Glossary of Terms), are charged with ensuring that those processing data under their authority comply with the spirit and detail of this document. Other important parties mentioned in this document are:

(a) Research Data Centre (RDC) - A place were research can be done on sensitive data such that the risk of disclosure is reduced by controlling who can have access, what data they can analyse and what outputs can be taken away. The RDC may be accessed physically or remotely using secure software

(b) Linkage Agent -a body that performs the matching of records belonging to individuals from two or more datasets to form a single linked dataset.

(c) Indexing service - maintenance of a population index based on UPI (unique patient identifier, e.g. CHI); addition of anonymised identifiers (referenced to UPI) to individual records for the purposes of linking these records across two or more datasets.

Each of these parties will be acting under the authority of a data controller or a Caldicott Guardian or will itself have such responsibilities. It is essential that each party knows and understands the capacity in which it is operating within the SHIP framework.

SHIP Guiding Principles and Best Practices

1. Public Interest

Principles

- Scientifically sound and ethically robust research is in the interest of protecting the health of the public.
- The objective of SHIP is to facilitate scientifically sound and ethically robust research through the appropriate use of health data.
- The rights of individuals should be respected with adequate privacy protection, while at the same time the benefits for all in the appropriate use of health data for research purposes should be recognised.
- Data sharing and use should be carried out under transparent controls and security processes, and the purposes and protection mechanisms should be communicated publicly and to oversight bodies/individuals with responsibility for data processing.
- The responsible use of health data should be a stated objective of all organisations adhering to this instrument.

Best Practice

- It is the data controller's responsibility to ensure the development of *transparent* policies that demonstrate their understanding of public interest and the basis upon which they will use and disclose health data; equally importantly this must include the protection mechanisms under which use will take place. It is possible that these policies may not be developed solely by data controllers, but in conjunction with others, e.g. lawyers, but ultimate responsibility for implementation of such policies will lie with the data controller. (See further Appendix 1).

2. Privacy

Principles

- Data controllers should demonstrate their commitment to privacy protection through the development and implementation of appropriate and transparent policies.

- Every effort should be made to consider and minimise risks of identification (or re-identification) to data subjects and their families arising from all aspects of data handling.

Best Practice

- Organisations involved in data sharing and use should have a designated officer responsible for addressing privacy matters. This might be the Data Controller or Caldicott Guardian or someone delegated to act on their behalf.

- Assessing privacy risks is an integral component of a data controller's responsibilities and should form a central part of their privacy policy. This process should include the identification of confidentiality, security and privacy risks of any data handling including linkages, storage and access considerations. [1]

- It is acknowledged that at times data controllers may not be able to fully assess privacy risks, especially prior to linkages, however they should still carry out an assessment that identifies potential risks based on the information they do have.

- Potential data recipients should also assess the impact on privacy prior to submitting data access requests and they should highlight any identified risks in order to discuss these with the data controller.

- Appropriate disclosure control should be applied to all outputs; this should be carried out under the authority and oversight of the designated privacy officer.

[1] The Information Commissioner's Office offers a handbook containing guidance for carrying out risk assessments, this can be accessed at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

3. Consent

Principles

- Personal data must not be used without consent unless absolutely necessary.
- Where possible and practicable, consent should be obtained from each data subject prior to the use and sharing of personal data for research purposes.
- The refusal of data subjects must be respected unconditionally.
- Where possible and practicable, individuals collecting data should adequately inform data subjects of all material issues relating to the storage and use of their data. Material issues are those likely to affect a person in a non-trivial way.
- Where personal data are used, the minimum amount of personal data should be used to achieve the stated objective.
- Where personal data are used, the reasons and justification for its use are adequate and clearly explained.
- Where personal data are used, every reasonable effort should be made to inform data subjects of the purposes of the use.
- Where obtaining consent is not possible/practicable, then (a) anonymisation of data should occur as soon as is reasonably practicable and/or (b) authorisation from an appropriate oversight body/research ethics committee should be obtained.

Best Practice

- Consent procedures should be designed to obtain free and meaningful consent, that is, data subjects must be given sufficient information to make a decision that reflects their genuine wishes, must be given the opportunity to ask questions and have these answered, and must not be subject to coercive measures.
- Where there is the prospect of future use of data that is unknown at the time of consent, then data subjects should be informed of the broad purposes for which the data might be used. These purposes will delimit the appropriateness of any future use.
- Where consent is not to be obtained, the reasons for this must be clearly articulated and adequately justified.
- Vulnerable populations should be given adequate protections with respect to their needs.

- Cultural/religious beliefs should be respected in the approaches that are employed to consent/refusal and data use. These should reflect the NHS obligations in relation to equality and diversity[2]

- Privacy notices used to inform individuals about the processing of their data must be sufficiently specific to be meaningful and must adequately reflect the range of purposes for which the data will be used. Reasonable effort must be made to draw these to the attention of data subjects. (See further ICO guidance on Privacy Notices[3])

[2] See further 'Equality and Human Rights in the NHS' accessible at http://www.pfc.org.uk/files/Board_Guide_2nd_print.pdf

[3] Information Commissioner's Office 'Privacy notices code of practice' accessible at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf

4. Anonymisation

Principles

- Researchers should normally only have access to anonymised data and be subject to an obligation not to attempt to re-identify individual data subjects (for clinical trials, see further 10 below).

- Where possible and practicable, data should be anonymised before linkage and use so as to minimise risk of re-identification of individuals.

- Where researchers cannot or do not intend to anonymise data and where consent for use of personal data has not been obtained, approval from an oversight body, e.g. Privacy Advisory Committee, must be obtained.

- Where data have been anonymised, authorisation should be obtained where there is a risk of re-identification; anonymisation does not remove the need for authorisation.

- Risk of re-identification must be assessed by a body/individual with the relevant expertise to make such judgments.

- Data controllers should determine and agree upon the appropriate level of anonymisation to be applied to any given dataset or linkage exercise.

Best Practice

- The appropriate level of anonymisation for each linkage should be agreed upon by all data sources and maintained by the linker i.e. the individual/programme responsible for combining data (see further Appendix X for access protocol)

- Where possible and practicable, data subjects should be provided with accurate information about the levels of protection afforded to their data by anonymisation as well as an account of the real risks involved.

- There should be a separation of functions between data controllers, RDCs, linkers, indexers and recipients of linked datasets.

- All users of data should have signed a Memorandum of Understanding with respect to data storage, use and protections of data subjects.

5. Authorising/advisory bodies

Data Controllers and Caldicott Guardians can authorise the use and sharing of data under their custodianship. Advice can also be sought from bodies such as the Privacy Advisory Committee for Scotland (PAC) or local research ethics committees on the appropriateness of specific requests to use or share data. Thus individuals and/or independent bodies can act in an authorising or advisory capacity with respect to data use and linkage.

Principles

- In all circumstances of data use where consent has not been obtained, and for all uses of data which are beyond those specified when consent was obtained, then (a) approval from an independent oversight body/research ethics committee should be obtained and/or (b) anonymisation of data should occur as soon as is reasonably practicable.

- Where neither anonymisation nor consent is possible or where obtaining new consent from patients is not reasonably practical, data controllers and Caldicott Guardians should obtain approval from an independent oversight body/research ethics committee before authorising use of the data.

- In order to uphold the principle of transparency, authorising bodies, such as data controllers and Caldicott Guardians, and advisory bodies, such as PAC and research ethics committees, should clearly articulate and make readily available the criteria and procedures by which they decide whether or not to sanction data use.

- In order to uphold the principles of transparency and good decision-making, all data use/access requests to authorising bodies should include (i) clear information on reasons for access, (ii) purposes of the analyses and (iii) measures to be put in place to ensure privacy risks are minimised.

Best Practice

- Decisions taken by authorising and advisory bodies should be publicly available and justified.

- Authorising/advisory bodies and responsible individuals alike should uphold the Nolan Principles on Standards in Public Life whilst carrying out their duties, namely - selflessness, integrity, objectivity, accountability, openness, honesty and leadership.[4]

- Authorising/advisory bodies which are constituted as a group should include members from diverse backgrounds who possess the necessary expertise to make appropriate and justifiable decisions on use/access.

[4] The Nolan Principles are elaborated in Appendix X.

6. Governance

Principles

- All aspects of data handling must be carried out in accordance with applicable legal frameworks and ethical principles. Where applicable, NHS policy documents and directives must be upheld.

- All practices, including all data linkages, shall be appropriately monitored and regulated by a relevant individual, organisation or governance body as appropriate. It is possible that these activities will be monitored at an individual and organisational level simultaneously. Data controllers are primarily responsible for ensuring such governance policies and procedures are in place and for making these policies and procedures available to research users and the public alike.

- There should be a clear distinction in roles between those carrying out linkages, analyses and those policing governance and enforcing sanctions.

Best practice

- All stakeholders and research users operating within the SHIP framework should familiarise themselves with, and comply with so far as is relevant, the ethical and legal obligations specified in the SHIP Scoping Report.[5]

- All stakeholders and research users should undertake the SHIP training online module on *Information Governance: Rights and Responsibilities*.[6]

- Where data are to be used for purposes other than those originally proposed, this should be appropriately regulated and should normally only involve anonymised data and should include input from an authorising and/or advisory body. Those involved with this oversight should have the relevant expertise to carry out such responsibilities.

[5] This report is available from the SHIP Website accessible at …
[6] To be developed in due course via the Edinburgh Law School eSCRIPT distance learning platform.

7. Access

Principles

- Provided appropriated oversight mechanisms are in place, data controllers and research users should participate in appropriate sharing of data resources within the health and non-health contexts.[7]

- Access policies should be developed in a transparent and open manner; these should also be subject to public scrutiny and review.

- Data should be held and used in a secure manner and should only be accessible to authorised personnel. All access to health data for research purposes should be documented and monitored appropriately.

- All data recipients should be appropriately vetted to ensure they have adequate training. Vetting procedures should be robust and transparent and proportionate to the requests made and the sensitivity of the data requested.

Best Practice

- Governance mechanisms should incorporate appropriate and transparent vetting methods for data recipients i.e. researchers.

- Recipients must possess minimum training requirements necessary to handle the data in accordance with basic legal/ethical principles in addition to any requirements specified in the relevant data sharing agreement.

- All individuals dealing with health data regardless of their roles must be made aware of these best practice guidelines as well as their obligations under the law. Normally the responsibility of informing these individuals rests with the data controller and/or the individuals' employer(s).

- All individuals dealing with health data regardless of their roles must sign confidentiality agreements with the data source e.g. the employing institution or other relevant source. Advice on the relevant parties can be obtained for the relevant data controller(s).

[7] It must be recognised that issues other than governance may constrain certain data controllers from participation in data sharing. In the NHS resources are a particular constraint, and will become even more so over the coming decade.

- Any conflicts of interest should be openly declared from the outset and brought to the attention of those responsible for oversight; these persons/bodies will determine the appropriate course of action to be taken.

- Appropriate vetting and training methods should be implemented for staff. In particular, staff members should receive role-appropriate training depending on the level of data handling their role requires. As a minimum, staff should be aware of their legal and ethical responsibilities.[8] Ideally, all staff, data recipients and research users should undertake the SHIP training online module on *Information Governance: Rights and Responsibilities*.[9]

- Staff should be instructed not to discuss their work in inappropriate or public places.

8. Trusted Third Parties

In circumstances where trusted third parties are involved in any aspect of data use, seeding, linkage or sharing then:

Principles

- There should be a clear distinction as to function between the linker, indexer and the data controller/data custodian/recipient; linkers should be seen as clear intermediaries responsible only for linking data.
- Linkages may only be performed by a party other than a trusted third party in instances where all data subjects have given consent for this (see clinical trials guidance below).

- Trusted third parties should satisfy necessary vetting and training requirements and should be recognised as being free from any conflict of interest.

Best practice

- Researchers should only pass on data beyond the limits of a sharing agreement where they are required to do so by the law e.g. public health and/or where accredited trusted third parties are to carry out linkage activities and appropriate authorisation has been obtained.

- Trusted third parties should conduct themselves in line with the Nolan Principles of Standard in Public Life, i.e. accountability, openness, selflessness, integrity, honesty and leadership.[10]

[8] ISD offer DP 'seminars' during staff induction and staff must sign documents each year stating they are aware of their DP responsibilities. Perhaps data handlers should carry out some kind of on-line training session/assessment. At the very least, they should sign a document acknowledging that they are aware of and agree to undertake their obligations.
[9] To be developed in due course via the Edinburgh Law School eSCRIPT distance learning platform.
[10] Sir Alan Langlands, Seven Principles of Public Life, for further instruction see 'Good Governance Standard for Public Practice' accessible at http://www.cipfa.org.uk/pt/download/governance_standard.pdf

9. Data Controllers and Data Processors

Principles

- Data controllers and data processors and their respective roles and responsibilities should be identified clearly from the outset and this should be articulated.[11]

- All personnel involved in a role as data controllers or data processors should be fully aware of their roles and responsibilities, including those contained in this document.

- These roles and responsibilities should be subject to robust governance mechanisms designed to ensure that these roles are being carried out appropriately and to the standards legally and ethically required.

Best practice

- There should be prior agreement between stakeholders about who will be a data controller (and a fortiori data processor) and on what basis.[12]

- Data controllers should develop and publish clear instructions on the policies and procedures according to which they will consider applications to use or share their data. These instructions should include lines of decision-making and accountability, terms and conditions, time scales for decisions, and any appeal mechanisms, where appropriate.

[11] The Article 29 Data Protection Working Party 2010 guidance on data controllers and data processors can be consulted for specific guidance.

[12] The NHS Scotland 'SWISS' database (Scottish Workforce Information Standard System) is a national repository of Scotland's workforce information.). The stakeholders have various needs for the same database and have agreed that they are data controllers in common i.e. they have a common interest in the resource but are separately liable for their own separate uses. Note, then, this is not the same as being jointly liable which would mean all stakeholders are responsible for all uses and breaches.

10. Clinical Trials

Principles

- Mechanisms for linkages involving clinical trials must permit re-identification by the principal data source, this is particularly important for pharmacovigilance purposes.

- The specific circumstances and conditions governing whether or not patients involved in clinical trials can be contacted and by whom, should be clearly set in place in transparent policies.

- Researchers should only seek to contact participants directly with respect to information arising from a clinical trial in which they took part where prior consent to be contacted for specific purposes has been obtained.

Best practice

- In limited cases, it may be desirable and permissible for those holding data arising from a clinical trial to perform a linkage; however this should only occur where patients have given explicit consent for extra information about them to be gathered by the researcher.

- Researchers should normally contact an intermediary i.e. the original data source, and request that they contact or arrange for contact with participants.

11. Cross-sector sharing

Principles

- Where ethical and legal standards are met, data should be made accessible to trusted researchers across disciplines. The value of such cross-sector sharing should be recognised.

- Along with the potential benefits of cross-sector sharing, risks should also be identified and appropriately addressed. In particular, assurance of reciprocal privacy standards across sectors is necessary.

- The unnecessary duplication of approval procedure(s) and governance mechanisms should be avoided. Mutual recognition of equivalent standard and procedures should be sought.
- Where data are to leave the European Economic Area (EEA), data controllers should ensure that equivalent data protection standards apply in the recipient country.

Best practice

- Clear and easy to understand specifications covering confidentiality, security and privacy, and which define roles and protocols, should be agreed prior to cross-sector data sharing taking place.

- Cross-sector data sharing agreements and requests should be considered by an appropriately constituted and competent oversight body.

- Systems of mutual recognition of governance and security arrangements should be established between sectors intending to share data.

12. Data sharing agreements

Principles

- Roles and responsibilities of parties to data uses and linkages should be identified from the outset, terms and conditions for data sharing should also be agreed upon in the form of a memorandum of understanding (MoU). (model agreement to be provided as an Appendix)

- Where researchers wish to deviate from/modify the terms of the data use/sharing agreement at any time, new terms must be agreed upon by all parties concerned and such changes should be monitored by the relevant oversight body/mechanisms.

Best practice

- All MoUs should include minimum conditions for data linkages reflecting legal and ethical obligations.

- MoUs should include details on the purpose for access, and intended uses of data, security measures put in place and the length of time for which data will be held. This time period must be justified.

- An undertaking should be given on the part of the Data Controller to supply particular data of particular accuracy by a particular time.

- An MoU should clearly identify the Data Controller(s) and should address how they will discharge their responsibilities, especially where multiple data controllers are involved. (see further Appendix X)

- Where multiple data controllers and/or data custodians are involved in a linkage and one (or more) demands special terms for inclusion in the MoU, individual arrangements can be kept separate, that is to say, all other data holders do not need to sign this particular MoU.

13. Public and stakeholder engagement

Principles

- Public and stakeholder engagement is an integral part of good governance. As far as possible, account should be taken of the full range of stakeholder positions in the development and implementation of governance arrangements.

- The interests of one (or a few) stakeholder(s) should not dominate use/linkages or the conditions of the same, especially where this might be at the expense of other stakeholder interests. Robust justifications must be given for any departure from this principle.

Best Practice

- Stakeholder interests and expectations should be monitored over time by an appropriate body or individuals with appropriate expertise for the task. Where necessary, governance arrangements should be adapted to take account of shifting stakeholder needs and expectations.

- Active engagement exercises should be developed and implemented over time to monitor and respond to stakeholder interests.

14. Sanctions

Principles

- Sanctions for failure to respect terms and conditions should be clearly stipulated in all data use/sharing documentation.

- Sanctions should be enforced by a body/individual independent to those granting permissions for access to data sets (i.e. data controllers) e.g. an independent body set up for monitoring/governing or the Information Commissioner's Office.

Best practice

- In order to identify which individuals are accountable at each stage of data processing/use/linkage/sharing, the following information should be documented: (i) who is permitted to access data, (ii) to what extent can they access the data, (iii) the status of data between transfers and between parties, (iv) whether or not data will be anonymised, where, how and by whom, and (v) the physical location of the data and security mechanisms put in place.

- Staff should always liaise with their local information governance (IG) team or designated officer responsible for IG. In the first instance, the Information Commissioner's Office can also be consulted where privacy concerns arise/guidance is needed.

- Different options for sanctions exist. These include (i) ICO sanctions (monetary fines), (ii) termination of data sharing agreements, (iii) legal action for breach of agreement [contract law], and (iv) an undertaking concerning future policy of non-data sharing with the individual/organisation in breach of obligations. Funders and publishers can also be informed of breach of data use/sharing agreements to serve as a deterrent.

15. Benefit Sharing

Principles

- Benefits arising from data use/sharing using health data are public goods and should be shared as widely as possible.

- The sharing of outputs and benefits arising from research under SHIP should be the norm and associated commitments should form part of data sharing agreements.

- Where linkages resulting in commercial gain are envisaged, this should be clearly articulated and widely communicated.

Best Practice

- Public entities or those receiving public funds should ensure that the results of research conducted using (partly or wholly) data under their custodianship are made publicly available either through publication or by other means.

- Data controllers should adopt the practice of publicising brief accounts of research done with their data sets, the parties involved and, where possible, the benefits produced.

- Likely and actual benefits should be identified as early as possible and every reasonable effort made to realise such benefits.

- Appropriate attribution should be given to those parties contributing the realisation of benefits.