University of Edinburgh
School of Law

Research Paper Series

No 2012/13

Information Governance of Use of Health-Related Data in Medical Research in Scotland: Towards a Good Governance Framework

Graeme Laurie and Nayha Sethi
Professor of Medical Jurisprudence and Research Fellow
Graeme.Laurie@ed.ac.uk, nayha.sethi@ed.ac.uk

Abstract

This paper is the second in a series addressing information governance challenges in health-related research involving patient data and it is set against the current legislative and common law landscape within the UK. In Working Paper No.1 we described the diverse actors, regulatory bodies and systems in place within the current framework, and critically examined their roles relative to the different ethical and legal issues at stake and the surrounding literature. In light of this analysis, we advanced a template for good governance: a series of questions relating to benchmarks and standards against which existing and emerging governance models can be assessed. We then evaluated the current governance landscape against these standards, highlighting key areas that required improvement, concluding with recommendations for change.

This paper moves one step further and examines more closely what it means to talk of good governance in the health-related research arena. We draw upon our research as part of the SHIP initiative[1] – a consortium working to build the Scottish Health Informatics Platform, funded by the Wellcome Trust and in partnership with NHS Scotland. We build on our academic findings and practical experience of working iteratively with key policy and practice stakeholders in the field to propose a new model of good governance in practice. In particular, we consider how guiding principles and best practice, in tandem with a good governance template, provide not only a good governance framework for SHIP but also an approach that is transformative of the ways in which health-related research is carried out and governed, both in Scotland and elsewhere.

The elements of good governance that we advance are set in the context of health data for research. It is important to note, however, that the lessons that can be learned from our work – and the model that we proffer - are applicable to a much broader range of governance settings, such as local authority and other public/private instances of data sharing. Our model adopts an approach of proportionate governance and is unique in this regard. It goes far beyond existing approaches to information governance in the research context while fully respecting relevant ethical and legal norms.

Keywords

Information governance; proportionate governance: personal data; good governance framework; patient identifiable information; secondary uses of data; health-related research; SHIP; health informatics; regulatory landscape.

[1] The SHIP Information Governance Stream comprises of the authors :

Graeme Laurie is Professor of Medical Jurisprudence and Director of Research at the School of Law, University of Edinburgh. Founding Director, The J Kenyon Mason Institute for Medicine, Life Sciences and the Law

Nayha Sethi is a Research Fellow and Doctoral Candidate at the AHRC/SCRIPT Centre, School of Law, University of Edinburgh, Deputy Director, The J Kenyon Mason Institute for Medicine, Life Sciences and the Law.

Contents

PART 1 - WHAT MAKES GOOD GOVERNANCE?

CHAPTER 1

1.1 Introduction

This paper is the second in a series addressing information governance challenges in health-related research involving patient data and it is set against the current legislative and common law landscape within the UK. In Working Paper No.1 we described the diverse actors, regulatory bodies and systems in place within the current framework, and critically examined their roles relative to the different ethical and legal issues at stake and the surrounding literature. In light of this analysis, we advanced a template for good governance: a series of questions relating to benchmarks and standards against which existing and emerging governance models can be assessed. We then evaluated the current governance landscape against these standards, highlighting key areas that required improvement, concluding with recommendations for change.

This paper moves one step further and examines more closely what it means to talk of good governance in the health-related research arena. We draw upon our research as part of the SHIP initiative – a consortium working to build the Scottish Health Informatics Platform, funded by the Wellcome Trust and in partnership with NHS Scotland. We build on our academic findings and practical experience of working iteratively with key policy and practice stakeholders in the field to propose a new model of good governance in practice. In particular, we consider how guiding principles and best practice, in tandem with a good governance template, provide not only a good governance framework for SHIP but also an approach that is transformative of the ways in which health-related research is carried out and governed, both in Scotland and elsewhere.

The elements of good governance that we advance are set in the context of health data for research. It is important to note, however, that the lessons that can be learned from our work – and the model that we proffer - are applicable to a much broader range of governance settings, such as local authority and other public/private instances of data sharing. Our model adopts an approach of

proportionate governance and is unique in this regard. It goes far beyond existing approaches to information governance in the research context while fully respecting relevant ethical and legal norms.

For a thorough discussion and analysis of the legislative landscape governing secondary uses of data for research, we refer the reader to Working Paper No. 1 in this series.[2] However for the purposes of this paper, and to set the context, we offer a brief overview of the issues explored, and the conclusions reached.

1.2 Issues identified in Working Paper No.1

We first identified the abundant literature base that reveals:

(1) The great potential which dataset linkage can offer within and beyond the health sector, and

(2) That the governance framework in its current state is impeding the realisation of such benefits.

We thereafter identified the key ethical and legal issues engaged in this setting as well as governance mechanisms that are commonly deployed; the most pertinent of these are the privacy interests and public interest(s) that are frequently weighed in balance, proportionality, choice (consent), anonymisation, authorisation and public attitudes and trust.

We then looked more closely at the reasons for the sub-optimal state of play, noting that confusing, uncertain and over-burdensome legislation and consequently disproportionate governance mechanisms pose key obstacles to research.

We established from our research a set of key questions reflecting benchmarks and standards against which to test current and emerging governance models: we named this our *governance template*. When we carried out this exercise, we concluded the following:

[2] Laurie G and Sethi N, 'Information Governance of Use of Health-Related Data in Medical Research in Scotland: Current Practices and Future Scenarios' (2011) University of Edinburgh Law Working Paper No. 2011/26 Accessible at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1946258

(1) A wide array of decision-makers are involved in approval mechanisms in Scotland with no obvious common frames of reference nor means of working in a way that is complementary to each other;

(2) Given the confusing nature of the law, it is doubtful that all relevant parties currently understand their legal and ethical obligations or the associated flexibilities within the law which allow sharing and linkage of data,

(3) An appropriate balance between consent, anonymisation and authorisation as mechanisms for information governance in health-related research is not currently being struck within Scotland;

(4) The current governance model is disproportionate when considering the relative benefits that can be realised from health-related research compared to the relative risks of pursuing that research with patient data. It is also disproportionate with respect to the number of governance mechanisms and decision-makers involved.

We have made several recommendations about how to improve the current landscape, in order to engender a more facilitative research environment without diluting appropriate scrutiny. These recommendations, alongside our governance template, inform our good governance framework, which we explore in depth here.

Key messages from this paper are:

- A clear account of a good governance framework is needed in order to facilitate the realisation of the great potential for secondary uses of data;
- All parties affected by the governance framework should possess a clear understanding of their responsibilities and the values and principles according to which they must guide their conduct;

- Due regard must be given to, and an appropriate accommodation arrived at, between the various ethical and legal considerations at stake – different governance mechanisms can be deployed alone or in combination to achieve this, and their relative merits and limits must be understood accordingly;
- A proportionate approach to governance is essential and necessitates a robust and reasonable assessment of relative benefits and risks as well as the establishment of mechanisms to safeguard against these risks and deal with their occurrence;
- Proportionate governance is a multi-faceted enterprise, including not only risk/benefit analysis, but also considerations of reputational risk and implications for public trust, the assessment of the relative merits of preferring certain governance mechanisms over others, and the need both to streamline approval mechanisms and to clearly define multi-level approval pathways with appropriate access conditions and sanctions.

CHAPTER 2 What makes good governance?

Key questions addressed by this chapter:

- What are the key components of a good governance framework?
- Why are each of these components so important, and what do they mean in practice?

Key Messages from this chapter

- A good governance framework is integral for smooth functioning and effectiveness within an organisation/sector
- Our good governance framework consists of 4 key components : (1) Guiding Principles and Best Practice; (2) Safe, effective and proportionate governance; (3) Roles and Responsibilities of Data Controllers and (4) Researcher Training
- Proportionality is an overarching principle which should be at the forefront of the construction of any governance framework
- A risk-based approach should underpin proportionate governance because this allows us to assess and to strike an appropriate balance between promoting important values and facilitating research in the public interest
- Authorisation is an effective governance mechanism for operationalising a proportionate, risk-based approach to governance, but this does not preclude a role for consent or anonymisation approaches; governance responses must be adaptable and proportionate to circumstances in every case.

The construction and implementation of a good governance framework is an essential component to any successfully functioning organisation.[3] Sir Alan Langlands's group has identified good governance as:

[3] The Independent Commission on Good Governance in Public Service (2004) 'The Good Governance Standard for Public Services'. See

> '…focusing on the organisation's purpose and on outcomes for citizens and service users; performing effectively in clearly defined functions and roles; promoting values for the whole organisation and demonstrating the values of good governance through behaviour; taking informed, transparent decisions and managing risk; developing the capacity and capability of the governing body to be effective and engaging stakeholders and making accountability real'.[4]

Good governance is particularly important in ensuring responsible and beneficial use of personal information within health research, where the potential risks and benefits of data linkage must be appropriately accommodated.[5] The Scottish Health Informatics Programme is dedicated to maximising the benefits of secondary uses of health data for research.[6] It represents an important step forward for research both within and beyond the medical setting. The programme facilitates and oversees the linkage of a vast range of data, thus gaining access to and being jointly responsible for a considerable amount of uses of Scottish population health data.

The solutions proposed for Scotland are not, however, restricted to her shores. Indeed, we believe that the analysis contained herein is in many senses universalisable to any number of jurisdictions facing the challenges of data linkage for medical research in the public interest. And, while the particular details of the model proposed here are adapted for Scottish purposes, the principles, considerations, approaches and the model of proportionate governance will have resonance far beyond Scotland.

---

http://www.cipfa.org.uk/pt/download/governance_standard.pdf; United Nations Economic and Social Commission for Asia and the Pacific 'What is Good Governance?' http://www.unescap.org/pdd/prs/projectactivities/ongoing/gg/governance.asp; International Monetary Fund (2005) 'The IMF's Approach to Promoting Good Governance and Combating Corruption — A Guide' see http://www.imf.org/external/np/gov/guide/eng/index.htm; Siddiqi S et al (2009)'Framework for assessing governance of the health system in developing countries: Gateway to good governance' in Health Policy Volume 90, Issue 1 , Pages 13-25,

[4] The Independent Commission on Good Governance in Public Service (2004) 'The Good Governance Standard for Public Services'. At page 4

[5] Department of Health, Research Governance Framework for Health and Social Care: Second Edition (2005) See http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4108962

[6] http://www.scot-ship.ac.uk/

Prior to laying out our good governance framework, we briefly discuss the methods which we have adopted in its construction.

Methods

We have employed several different methods in order to develop the framework. Most notably, we adopted an iterative, multidisciplinary and discursive approach through our collaborative working in SHIP. We worked together with academics from different disciplines to our own, including in particular, sociologists involved in public engagement and health researchers experienced in analysing linked health datasets.

Additionally, we have had continuous access to key policy and practice stakeholders within and beyond colleagues involved in SHIP. This has included Information and Statistics Division in NHS Scotland which acts as custodian to a large amount of Scottish population health data and other influential bodies involved in safeguarding data, authorising and approving data access applications including Caldicott Guardians and the Privacy Advisory Committee for Scotland (PAC). They have fed into and responded to our findings on an on-going basis and allowed us to refine our model accordingly.

We have tested our evolving thinking with the researcher community, the wider public and Local Authorities who are responsible for sharing information for cross-sectoral linkage. We have held and participated in various meetings bringing together those interested in health research and data linkage not only on a Scottish or UK-wide basis, but on an international level.

We have presented our good governance framework at different stages of its development, gaining valuable interest and feedback from international as well as local actors and stakeholders. We have led the SHIP Information Governance Working Group[7] that resulted in the formulation of SHIP Guiding Principles and

[7] The membership of the group included: Peter Craig (Chief Scientist Office, Scottish Government), Muriel Douglas (Head of NHS Central Register) Andrew Morris (Professor of Medicine, Director Medical Research Institute. University of Dundee.) ; Janet Murray (Consultant in Public Health Medicine and Caldicott Guardian, Information Services Division NHS Scotland) ; Patricia Ruddy (Data

Best Practice[8] as well as a pathway for application approvals (discussed in Chapter 3) and case study analysis. We have been developing and continue to run a pilot programme in order to test the efficiency of, and improve upon our SHIP Researcher Training Package. This approach has enabled us to refine our governance framework to ensure that it is functional, effective and responds to the needs of key actors and stakeholders, including researchers themselves.

However, the very processes of engagement, consultation and inclusion of recommendations from these individuals and bodies is in its own right, an important method; it has allowed us to establish, develop and maintain a spirit of collegiality and collectiveness and ultimately, it is hoped, a degree of buy-in which is necessary for consistent adoption and implementation of the framework across the landscape.

Further, we have worked closely with SHIP's Public Engagement work stream. To date, it has carried out research on public attitudes to data sharing for research purposes and revealed important insights. For example, the focus group findings indicated that control, confidentiality and trust were important considerations[9] and we have kept this in mind throughout the development of our good governance framework. Equally, we suggest that our proposals could inform on-going public and stakeholder debate about what counts as appropriate governance mechanisms over data sharing and linkage and how these can be further informed by public and stakeholder engagement.

Finally, our good governance framework has gone on to inform the SHIP Blueprint which is intended to guide researchers, Caldicott Guardians, data

---

Protection Advisor, NHS National Services Scotland); Steve Pavis (Head of Programme, Information Services Division NHS Scotland) ; Anthea Springbett (Programme Principal (SHIS-R), Information Services Division NHS Scotland) ; Violet Warwick (Scottish Health Informatics Programme Manager) Graeme Laurie (Director of AHRC/SCRIPT Research Centre, School of Law, University of Edinburgh) , Nayha Sethi (Research Associate, AHRC/SCRIPT Research Centre, School of Law, University of Edinburgh)

[8] SHIP Guiding Principles and Best Practice, see : http://www.scotship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf

[9] Publication forthcoming, authored by Cunningham-Burley S, Laurie G, Pagliari C, Aitken M, Sethi N

controllers and the wider community with a 'strong, clear and efficient' model for linking health data within and beyond the health sector. [10]

2. Proportionate governance: the model and the key components inherent in a good governance framework

Here, we advance what, as a result of our research, constitutes a good governance framework. This is composed of four key components:

(1) Guiding Principles and Best Practice
(2) Safe, effective and proportionate governance
(3) Roles and responsibilities of Data Controllers
(4) Researcher training

We now discuss each component in detail, explaining its origins and justifying its inclusion and suggesting why such a model of *proportionate governance* is so important in the achievement of good governance.

2.1 Guiding Principles and Best Practice

First and foremost, a good governance framework needs to include an overt statement of the values and standards according to which activity will be assessed.[11] This must be accessible and sufficiently adaptable to be adopted and implemented across all levels of decision-making and by all actors involved in the process. We believe that guiding principles, accompanied by instances of best practice provide the best means for ensuring this.

Principles are recognised as being flexible enough to be adopted in a wide range of settings by diverse actors with diverse responsibilities, whilst simultaneously

[10] SHIP: A Blueprint for Health Records Research in Scotland: Draft for consultation (2011) see http://www.scot-ship.ac.uk/sites/default/files/Reports/SHIP_BLUEPRINT_DOCUMENT_draft_for_consultation_081211.pdf

[11] Banff Executive Leadership Inc (2004) 'Improving Governance Performance: Rules-Based vs Principles-based Performance' in Leadership Acumen Issue 16 Jan/Feb 2004; Julia Black, 'Forms and Paradoxes of Principles Based Regulation', LSE Working Papers 13/2008

providing enough content to guide individuals as to the key values and considerations that should be factored into decision-making processes[12], such as whether data should be made available for sharing, whether institutional arrangements are sufficiently robust to accommodate data sharing and whether appropriate governance mechanisms are in place for such sharing.

2.2 Safe, effective and proportionate governance

Proportionality is a key concept not only within our good governance framework, but which features across a diverse range of legal spheres. In particular, it plays a significant role within Human Rights, European and private law. As a principle that underpins European law, it implies that governments should refrain from taking action beyond that which is necessary in achieving specific ends of the government.[13]

Adopting a proportionate approach to governance has many benefits; it ensures that any measures taken, (whether in terms of sanctions for breaches/non-observation of key standards, or anticipatory measures in place to assess risks within an organisation or across a regulatory landscape) correspond to the gravity of any breaches (actual or anticipated). This is likely to engender a culture of compliance, rather than caution, the latter environment being one where those governed act conservatively, for fear of disproportionate sanctions or over burdensome regulatory mechanisms. Further, proportionality is a concept that can be applied to manifold settings by different actors and at different levels of decision-making.

However, it is not without its limitations, it has been suggested that within the Human Rights setting, for example, proportionality does not, in itself, guarantee

[12] Beauchamp T and Childress J (2008) 'Principles of Biomedical Ethics' Sixth Edition, Oxford University Press; Seligman C, Syme G, Gilchrist R (1994), 'The Role of Values and Ethical Principles in Judgments of Environmental Dilemmas ' in Journal of Social Issues Volume 50, Issue 3, pages 105–119, FSA (2007) 'Principles Based Regulation: Focusing on the Outcomes that Matter', Commissioner McCreevy (2007), 'Capital Market Place' in Wall Street Journal 5th March 2007, available at http://www.eurunion.org/newsweb/EUInMedia/cmcWSJoped030507.htm

[13] Harbo T, (2010) 'The Function of the Proportionality Principle in EU Law' in European Law Journal Volume 16, Issue 2, pages 158–185

supremacy of Human Rights law. [14] Notwithstanding, the rights culture in which we live requires that any interference with individual rights be justified and legitimate. While interference might on occasion be permissible, this must be within strictly controlled terms. Thus, for example, under the ECHR paradigm interferences with the right to respect for private life can only be upheld if they are necessary and proportionate to advance a specific social end. [15]

In the European context, it is widely accepted that a proportionate measure implies that 3 key elements are satisfied:

1) The measure is appropriate;
2) The measure is necessary and
3) The measure is proportionate to the objective.[16]

It has been argued that proportionality is not always interpreted consistently by different member states, and that its terms are vague.[17] However, these are criticisms to which all principles are subject[18] and which rules cannot escape either.

It has also been argued that in reaching decisions about what course of action should be taken, judges are less likely to rely upon proportionality as a concept, and its 3 components mentioned above, and more so upon the extent to which they are "prepared to defer to the choices of the authority that has adopted the measure at issue."[19]

[14] Ciancardo J, (2009) 'The Principle of Proportionality : its Dimensions and Limits'
[15] The Rt. Hon. Lord Justice Stanley Burnton, 'Doctors, Patients and the Human Rights Act' Medico-Legal Journal (2011) Vol. 79 Part 4, 115–128.
[16] Craig P and De Burca G, 'EU Law: Text, Cases and Materials', 4th edn., 2007. Oxford: OUP
[17] Walter van Gerven, *The Effect of Proportionality on the Actions of Member States of the European Community: National Viewpoints from Continental Europe, in* The Principle of Proportionality in the Laws of Europe (Evelyn Ellis ed., 1999);
[18] See in particular Black J, 'Forms and Paradoxes of Principle Based Regulation' LSE Law, Society and Economics Working Papers 13/2008 accessible at: http://eprints.lse.ac.uk/23103/1/WPS2008-13.pdf and 'The "Principles" Paradox' (March 1, 2008), Duke Law School Legal Studies Paper No. 205 Available at SSRN: http://ssrn.com/abstract=1121454
[19] Gunn T, 'Deconstructing Proportionality in Limitations Analysis' in Emory International Law Review, Vol 19 (2005) 465 - 498

We suggest that our good governance framework will counter the last two criticisms by:

(a) offering clear articulation, examples of, and manifestation of what it means to adopt proportionate governance in the health information research context – this promotes clarity and consistency of approach, and

(b) ensuring that decision-makers conduct transparent assessments of the risks/benefits and governance options available, which must be justified both as proportionate and by reference to the principles and best practices discussed above.

As we can see that proportionality occupies space far beyond the health setting. Proportionality is the overarching principle that ties the varying components of good governance together and should be the ultimate benchmark against which to assess the appropriateness of conduct – both at the level of individual linkage decisions and the choice of what counts as appropriate governance over those linkages. Furthermore, it is proportionality which ensures that the different and sometimes competing considerations and values at stake are given due regard - neither over-excessive consideration nor insufficient attention. This is important in a field where there can be a tendency to polarise the acceptability of governance options – either consent *or* anonymise[20] – and this is unhelpful for failing to uncover what is truly at stake and how we might best proceed.

The need for proportionality is already reflected within some aspects of the existing and emerging regulatory landscape; the proposal for a new EU Data Protection Regulation[21] acknowledges the importance of proportionality: *'The principle of proportionality requires that any intervention is targeted and does not*

[20] Academy of Medical Sciences, (2006) 'Personal data for public good: using health information in medical research'. See http://www.acmedsci.ac.uk/p48prid5.html

[21] Proposal for a new Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final accessible at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Note mention of proportionality also appears in draft recitals 133 and 139 and also draft Article 22(4).

go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal, from the identification and evaluation of alternative policy options to the drafting of the legislative proposal'.[22] Articles 81-83 of the proposed new EU DP Regulation are directly concerned with health and research and we will discuss the related implications in our next working paper.

How might proportionality work in information governance?

For the purposes of secondary uses of health data for research, proportionality acts as a temper in two key ways: (i) alongside the balance which must be sought between individual privacy and the public interest – whereby it must be shown accordingly to the proposed new EU DP Regulation that use of personal data is necessary and proportionate to further a legitimate end such as the protection of the health of others, (ii) another balance must be struck in a much broader sense, viz, the balance between the privacy risks associated with data linkage and/or sharing and the corresponding governance mechanism set in place.

This last point requires further elucidation. The claim is that the principle of proportionality dictates that the level of scrutiny to which an action such as data linkage is subjected should be commensurate with the level and nature of the risks to which the said action may give rise. For example, if a researcher wishes to link datasets where patient identification is a highly unlikely outcome, then they should not be subjected to the same level of scrutiny (or restrictions) as a researcher wishing to link datasets with a higher possibility of identification.

Equally, to require that particular governance mechanisms are put in place – for example to require the explicit consent to linkage be obtained from each data subject – might be judged disproportionate to the level and nature of the interests at stake, for example where adequate security provisions are in place. Conversely, proportionate governance equally requires that where there is a high risk of re-identification/disclosive output or other form of harm resulting from a linkage, there should be a higher governance burden to meet.

[22] Ibid at section 3.2 Subsidiarity and Proportionality

Proportionality – linked to accurate and appropriate risk assessment – is a key feature of good governance. Thus, how we perceive and classify risk is an important factor, and we move on to discuss this in the next section.

2.3 A risk based approach

SHIP foresees the great research potential of cross-sectoral linkage, which would likely lead to access to, and joint responsibility for, a wide-range of linkages of population data, including police, social care and childhood data. For the purposes of this paper, we focus discussion on the risks as they relate to health data, appreciating that linking data from alternative sectors e.g. police and social care, will bring additional challenges which we will address in future papers.

(i) Moving from an implicit to explicit approach to risk

As it stands, the UK Data Protection Act 1998 (DPA)[23] does not take an overtly risk-based approach to data processing. Rather, it places emphasis on the fair and lawful processing of data, and processing 'where necessary' as reflected in the first DP Principle.[24] This being said, risk does appear indirectly within the legislation by virtue of the way in which personal data are defined; the likelihood of identifiability represents a means of identifying a level of risk associated with processing the data, and accordingly, we would expect data controllers to respond depending on whether or not they think they are or are likely to be dealing with personal data. Arguably, it is an implicit risk approach rather than an explicit one.

Indeed, the same could be said of anonymisation – which is not an absolute and more an art than a science. The key aim is reducing risk and bringing risk below an acceptable threshold. What we are suggesting here is that we need to move more overtly from an implicit approach to risk to an explicit one.

[23] For a comprehensive overview of the legislative landscape governing secondary uses of data for health research see Laurie G and Sethi N, 'Information Governance of Use of Health-Related Data in Medical Research in Scotland: Current Practices and Future Scenarios' (2011) University of Edinburgh Law Working Paper No. 2011/26 Accessible at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1946258

[24] Iverson A et al (2006) 'Consent, Confidentiality and the Data Protection Act' in British Medical Journal 332:165

Risk features as a dominant consideration throughout the proposed new EU DP Regulation[25]. Proposals for reform, if implemented, could mean that the legislation is more in keeping with our own proportionate governance model which views a risk-based approach as an essential element of good governance. In order for such an approach to be realised, it must fit with an appropriate governance model, we discuss this next.

(ii) An appropriate governance model for a risk-based approach

Within the health setting, data used for research are deemed sensitive data under data protection law, and thus necessitate that additional requirements are met before data processing is lawful. That is, under the UK Data Protection Act (1998), at least one condition in both Schedule 2 **and** Schedule 3 must be satisfied.[26] Despite the requirement of an extra condition being imposed, flexibility is not lost; it is merely an example of proportionality in action: an extra requirement due to the sensitive nature of the data in question. Similarly, whilst consent appears in both Schedule 2 and 3, this does not necessarily imply that we should consider consent as the optimal or proportionate means by which to regulate data processing.[27] Consent is neither necessary nor sufficient for processing of personal data under the Directive.

Notwithstanding, the 'consent or anonymise' approach has received significant attention as a governance model.[28] That is, where consent for the use of personal data for research could not be or was not obtained, the default position is to

[25] 'In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected': N66 within preamble of 'Proposal for a new Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012)

[26] Data Protection Act (1998)

[27] Al-Shahi R, Warlow C (2000) Using patient-identifiable data for observational research and audit. BMJ 2000;321:1031-1032,

[28] Academy of Medical Sciences, (2006) 'Personal data for public good: using health information in medical research'

anonymise the data prior to research use i.e. data sharing and linkage.[29] However, the model has been accused of impeding research.[30]

What has frequently been overlooked and subjected to far less robust scrutiny is an alternative to the consent or anonymise approach: authorisation. Authorisation is the governance model which has received least attention to date, and possibly, one that has been considered an inferior governance mechanism in comparison to consent and anonymisation models. Proportionate governance casts the role and potential of authorisation under a different light by considering it as a range of options that can be used alone or in combination with consent and or anonymisation.

Authorisation involves an individual/body making a decision about whether data should be shared (and in what form) when it is neither possible nor practicable for the data subject to input to the process. Caldicott Guardians[31], for example, when approached with data access requests, are responsible for deciding whether Health Board data for which they are responsible should be shared and whether or not it needs to undergo anonymisation or whether consent should be sought. The Privacy Advisory Committee in Scotland[32] (PAC) acts in a similar capacity – albeit it lacks statutory powers and is only advisory. None the less, its decisions carry considerable weight when advising on the suitability and conditions for linkages involving ISD/NRS[33] datasets.

[29] However, it is important to note both the National Health Service Act 2006 (by virtue of s 251 whereby the Ethics and Confidentiality Committee can lay aside the common law duty of confidentiality) and the de facto approach of the Privacy Advisory Committee for Scotland, have considered authorisation as a governance model.

[30]Strobl J, Cave E and Walley T (2000) 'Data protection legislation: interpretation and barriers to research'; *British Medical Journal* 321, 890–2.; Peto J, Fletcher O and Gilham C (2004) 'Data protection, informed consent and research: medical research suffers because of pointless obstacles' (editorial), *British Medical Journal* 328, 1029–30; Academy of Medical Sciences, 2006; Haynes CL, Cook GA and Jones MA (2007) 'Legal and ethical considerations in processing patient-identifiable data without patient consent: lessons learnt from developing a disease register', *Journal of Medical Ethics* 33, 302–7.

[31] NHS NSS Caldicott Guardians, see :
http://www.nhsnss.org/pages/corporate/caldicott_guardians.php

[32] NHS NSS Privacy Advisory Committee see :
http://www.nhsnss.org/pages/corporate/privacy_advisory_committee.php

[33] (ISD) Information Services Divisions of NHS Scotland is custodian of a vast range of NHS health data, and NRS is the National Register for Scotland.

In order for authorisation to be effective, it is essential that the authorising or advisory body or individual has a thorough understanding of the relative risks associated with any given data linkage, as well as the different legal and ethical considerations at stake. What should not be overlooked is that authorisation does not preclude other governance mechanisms such as consent or anonymisation being deployed. Rather, it provides an opportunity to determine the most appropriate mechanisms to be used and standards to be met for different linkage applications. This can give rise to diverse approval requirements; ones which proportionality would dictate should be relative to the benefits and burdens involved.

Authorisation represents a move away from the binary 'consent or anonymise'[34] model. PAC for example, has an expectation that consent will be obtained where identifiable patient data are used. Whilst the advisory body recognises that this is not always possible, it holds that *'in such circumstances, a clear explanation and justification should be given'*.[35] Amongst other things, explanations/justifications may include, for example: demonstrations of the scientific validity of a particular proposal; presentation of a strong case for why obtaining consent is not practical; evidence that privacy risks are minimised as far as possible and that adequate security measures are in place.

In Scotland, in addition to PAC, the Community Health Index Advisory Group (CHIAG)[36] also holds a key advisory role in relation to patient demographics and research uses. In each of these cases, the approach is similar: where consent or anonymisation are shown not to be viable options the authorising body takes on a scrutiny role to consider the risks and benefits of linkage/use and to recommend an acceptable outcome. Where linkage is approved, then often additional terms and conditions can be imposed, for example, additional security measures or a reduction in access only to necessary datasets essential to answer the research questions.

[34] Academy of Medical Sciences Response to Data Sharing Review – see www.acmedsci.ac.uk/download.php?file=/images/publication/...pdf

[35] NHS National Services for Scotland, Privacy Advisory Committee for Scotland 'Guiding Principles and Policy for Decision-making and Advice' accessible at http://isd.scot.nhs.uk/isd/files/PAC-Guidance-on-decision-making.pdf

[36] Community Health Index Advisory Group. See http://www.shsc.scot.nhs.uk/shsc/default.asp?p=108

Thus, authorisation (whether alone of in tandem with consent and anonymisation) complements a proportionate risk based approach to reviewing data linkage applications.

(iii) How to operationalise a proportionate and risk-based approach via authorisation

Reflecting on the potential risks to data subjects and, indeed, to data controllers, facilitates a proportionate approach to governance; it enables authorising bodies/individuals to impose safeguards or mechanisms which appropriately reflect the likelihoods of breaches and the nature of those breaches. Risk-based approaches offer a more bespoke and therefore more intuitive approach to governance. A fuller range of flexible and responsive governance mechanisms are at our disposal, to be deployed appropriately and after a suitable risk-based approach of what is at stake.

We now turn to consider the different elements which we consider key within a risk based approach.

2.3.1 Key elements of a risk-based approach

What does a risk-based approach involve? It requires not only the consideration of the relative risks associated with each proposed linkage, but additionally, ensures that important risk-related benchmarks are met.

These benchmarks include:

- the public interest
- safe data
- safe people
- safe environment
- consideration of relative risks

In this section, we explore each of these benchmarks and factors of relative risk.

Public interest

We start from the premise that scientifically sound, ethically robust research is in the public interest. We acknowledge that it is a term which is very difficult to define but in this there is some degree of strength in governance terms.[37] We consider it incumbent on a governance framework to promote a defensible view of public interest and to require applicants to demonstrate sufficiently that their research promotes public interests, or at least has a reasonable likelihood of doing so. It would be inappropriate and unduly restrictive to be prescriptive about what counts as public interest, but its importance in a governance framework reminds regulators and applicants alike that it is the paradigm threshold consideration which – if not met – will automatically result in rejection of a research proposal.

The Privacy Advisory Committee for Scotland (PAC) offers a helpful definition of public interest in this context - where there is 'a pressing social need or such reasonable likelihood that it will result in tangible benefits for society'.[38] PAC also points out that when considering the use of patient identifiable information for medical research, 'public interest' should be interpreted 'both to encourage good medical research[39] and 'to protect patient privacy'.[40]

Safe data

It is paramount that data are handled with due regard to privacy protection.. It has been widely acknowledged within the literature that data can never completely be anonymised so as to render identification of the individual

[37] Clark, S and A Weale. 2011. "Information Governance in Health: An Analysis of the Social Values Involved in Data Linkage Studies." The Nuffield Trust Available at: http://www.nuffieldtrust.org.uk/sites/files/nuffield/information_governance_in_health_-_research_report-_aug11.pdf

[38] NHS NSS Privacy Advisory Committee for Scotland, 'Guiding Principles and Policy for Decision-Making and Advice' accessible at http://www.isdscotland.org/isd/servlet/FileBuffer?namedFile=PAC-Guidance-on-decision-making.pdf&pContentDispositionType=inline

[39] It should be noted that in England, s251 National Health Service Act 2006 offers a legal decision-making basis for 'public interest'-oriented medical research. See http://www.opsi.gov.uk/acts/acts2006/ukpga_20060041_en_1

[40] Ibid

impossible.[41] However the process does render identification highly improbable, with the risk of identification still remaining. It should also be noted that anonymisation, like consent, is a device for respecting the interests of individuals.[42]

Where anonymisation is a pre-requisite for data-sharing, this should be carried out. The Caldicott principles[43], which relate to the use of patient identifiable information for treatment as well as research, stress that use should be restricted to the minimum amount of identifiable information necessary. [44]

It is however, also acknowledged that anonymisation has the potential to impede legitimate research by rendering the data less valuable i.e. robbing them of their 'richness'.[45] In instances where it is argued that anonymisation is inappropriate, PAC requires an explanation and justification for not anonymising data. Thus, safe data does not necessarily mean anonymised data in every instance, rather it means data subject safety mechanisms e.g. processes and terms and conditions, which correspond in a proportionate way, to the specifics of each application.

Safe data as part of a governance regime means ensuring that the mechanisms in place are sufficient and effective. That means that data should be adequately protected in a manner corresponding with its sensitivities, but this should not be to the extent that it renders data inaccessible or extremely difficult to access for important research purposes. The use of safe havens, as a central feature of SHIP,

[41] 'Absolute 100% anonymity is almost impossible to achieve without the data set being reduced to one data item, rendering it of little use for most research purposes' Confidentiality & Security Advisory Group for Scotland (2001) 'Protecting Patient Confidentiality: A consultation paper, Seeking Consent' http://www.csags.scot.nhs.uk/ppc/ppc.pdf.
See also Paul Ohm 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' 57 UCLA Law Review 1701 (2010)

[42] Laurie and Sethi (2011)

[43] The Scottish Government, 'NHSScotland Caldicott Guardians : Principles into Practice', see : http://www.scotland.gov.uk/Publications/2011/01/31115153/1

[44] Dame Fiona Caldicott is currently leading a review on the balancing of protecting patient identifiable information and sharing information for improving patient care, for more information, consult the Department of Health Website, see : http://www.dh.gov.uk/health/2012/02/dame-fiona-caldicott-to-lead-confidentiality-review/

[45] See note 41

is one way of assuring the safe data criterion and so minimising the governance burden.[46]

Safe people

The individuals processing the data at all stages of the data life-cycle must be aware of their respective responsibilities and act in accordance with them. This involves ensuring that effective training methods are implemented and that agreement is reached from the outset identifying who is responsible for the data at the different stages of the cycle. Data controllers in common will share joint responsibility, as it is not unusual that more than one individual is involved, however they might elect one individual as being responsible. A good governance framework must, accordingly, have clear articulation of lines of responsibility and accountability as well as an appropriate training and accreditation scheme for applicants to help to ensure that good governance principles for data handling are met (discussed further in Chapter 3).

Safe environment

It is paramount that adequate security measures are in place in order to safeguard the data. This includes consideration of where the data will be held, who has access to it, whether it will be transferred and under what circumstances, and for how long and where the data will be retained. Once more, it is important that those involved are aware of the security measures which they must observe. Some data may be required to be held and accessed within a safe haven, other lower risk data may be appropriate for travel to the researcher's institution, so long as that institution in turn is acceptable as a safe environment.

Again, proportionality is a key concept here; it would be onerous to require researchers to travel to a safe haven in order to link data that are already available in the public domain. Conversely, it might be deemed inappropriate to transfer highly sensitive data for linkage outside of a safe haven, due to the risks involved. The safe haven model is, therefore, another means by which the

[46] For more information on the safe haven approach, see the SHIP Blueprint (particularly pages 11 - 16) on the SHIP website, accessible at: http://www.scot-ship.ac.uk/

delicate considerations can be appropriately managed. By the same token, it should not be thought that a safe haven approach is suitable for all types of research or data linkage.

Relative risks

The benchmarks above, namely public interest, safe data, safe people and safe environment must be taken in to consideration for the duration of the data processing – both in their own right and cumulatively. The value of this benchmarking is to perform an early screening of the level of risk of any given application. If any of the five benchmarks is not satisfied, then an application should be subject to full scrutiny by an appropriate body such as the Privacy Advisory Committee in Scotland or equivalent.

If, however, the application clears this benchmark stage, then a Risk (privacy) Impact Assessment should be carried out to decide which level of scrutiny and terms and conditions should follow for each application.

2.3.2 Risk (privacy) Impact Assessment

The identification and appropriate weighting of likely risks involved in any given research application to link or share data is a further means to determine which of a range of possible governance pathways is most appropriate and proportionate to the aims that are sought. The proposed new EU DP Regulation recommends that data controllers include the implementation of data protection impact assessments as part of the measures taken to ensure compliance with the regulation.[47]

While not exhaustive, it is proposed that the following elements of risk should be given due consideration in any risk assessment:

[47]Article 22 s2 (c) Proposal for a new Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012)

(i) Privacy (the nature and likelihood of a breach of privacy) - This involves reflecting on the nature and likelihood of a breach of privacy and the considerations relating to privacy discussed above, including striking a balance between justified encroachment on privacy interests and the promotion of the public interest in research. It also implies a more technical consideration of anonymisation and of whether data will become potentially disclosive and if so, to what extent.

(ii) Impact of any privacy breach - It is important to take into consideration the impact which a breach could have on the data subjects, as well as the custodians of the data sets which have been linked. Thus, two key considerations in a privacy impact assessment are (a) the likely disclosiveness of any data linkage, and (b) the sensitivity of the data being handled.

(iii) Reputational impact for DCs of the application being approved - Due regard must be given to the impact that a linkage might have on the organisation and the individuals responsible for the approving it. This ties to consideration of public expectations of data use (discussed below). Data controllers and data custodians must consider the consequences of approving applications, particularly where there might be some impact upon their reputation and the trust bestowed upon them by the public, as well as researchers. For example, ISD, the Information Statistics Division for Scotland, part of NSS NHS is the custodian of many major health datasets in Scotland. They operate a robust mechanism of approvals including a role for a Privacy Advisory Committee to advise on issues such as these.

(iv)Research motive, e.g. commercial or other sensitive areas - Whilst data controllers are encouraged to facilitate data sharing for research, and to view this as being in the public interest, there are also situations where linkage of data will raise question about whether it in the public interest. This could include, for example, research into controversial areas such as intelligence linked to racial groups or where the research is done with a view to generating excessive

commercial profit. If any such concerns are raised, then they should be escalated to full review for further consideration.

(v) Public expectations including public interest value of research - This involves further reflection upon whether the study would promote or compromise the public interest. Public expectations are important and a good governance model recognises this importance and builds it in to its core considerations. Good governance is also anticipatory and avoids damaging or compromising public expectations or trust the value of research. Once again, if there are reasons to suspect that public expectations will not be met by a particular data linkage, there should be escalation of the application for full review.

2.3.3 Categories of Application

As the immediately previous discussion suggests, our model of good governance as proportionate governance seeks to assess different types of applications for data linkage and match them to appropriate governance pathways.

Allocating data accessing applications different categories for the approval process allows applications to be dealt with in a streamlined and proportionate manner. It would allow researchers to anticipate and thus prepare for the level of scrutiny against which their data access applications would be assessed. Additionally, it would ensure that data is shared according to terms and conditions that are neither overly onerous nor inadequately lax for the linkage in hand and the risks associated to it. We discuss this further in Section 3 below.

2.4 Roles and Responsibilities of Data Controllers

One of the key criticisms of data protection legislation, both at the European and UK level has been the uncertainty surrounding roles and responsibilities of data controllers and processors, particularly post-data linkage/transfer.[48] It is therefore integral that all actors involved in data processing have a clear

[48] Information Commissioner's Office (2009) 'A Guide to Data Protection' see http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf

understanding of, and where required, reach agreement upon who is responsible (whether jointly or individually) at every stage of linkage. We discuss this further below in Chapter 3.

2.5 Researcher training

Researcher training which offers a coherent and complete overview of legal and ethical issues involved with data linkage, as well as a clear articulation of the roles and responsibilities of researchers is integral to improving the governance landscape. Training should be easily accessible and developed with not only researchers, but the wider research community in mind. It should strive to instil confidence within the research community as to the different opportunities as well as duties to which data linkage gives rise.

Appropriate vetting mechanisms should also be in place and should be designed in such a way as to ensure (as far as possible) that valuable data does not fall into the hands of individuals who are insufficiently equipped to handle it and fulfil their responsibilities. We discuss this in more detail in Chapter 3 at 3.5

2.7 Conclusion

We have now laid out our key elements of our good governance framework and one dominant theme resonates throughout the discussion: good governance is proportionate governance. Good governance recognises the preceding considerations, and attempts to incorporate them into a governance framework, it also anticipates the potential risks and has processes in place to prevent them from happening, and to manage and minimise the damage when they do take place. A good governance framework will do all of this proportionately, that is, it will both anticipate and react to possible risks, and actual breaches in a manner which adequately reflects the likelihood of the risk and the damages associated.
Good governance also links the appropriate governance pathway to different kinds of applications – acknowledging their diversity and properly taking into account a full range of considerations. It avoids one size fits all while also equips

decision makers with the tolls, language and governance device to take apply the most appropriate governance framework.

Key messages from this chapter are :

- Through our collaborative work with SHIP, we have adopted an iterative, multidisciplinary and discursive approach in developing our good governance framework.
- Our good governance framework consists of 4 key components: (1) Guiding Principles and Best Practice; (2) Safe, effective and proportionate governance; (3) Roles and Responsibilities of Data Controllers and (4) Researcher Training
- Guiding principles and instances of best practice are an effective way of articulating the values and principles which should be respected throughout an organisation, as well as how these can be implemented in practice.
- Key elements of safe, effective and proportionate governance include: proportionality; a risk-based approach; guiding principles and best practice, public engagement and vetting and training methods.
- Proportionality should feature as a dominant over-arching theme of good governance; it involves allocating precautionary measures and disciplinary mechanisms which appropriately reflect the perceived risks or damages of actual breaches**.**
- A risk-based approach provides the most suitable approach to operationalising proportionate governance. It involves consideration of key risk-related benchmarks which include: the public interest, safe data, safe people, safe environment, consideration of relative risks when these elements are considered together
- A more specific risk assessment then follows which includes 5 elements: risks associated with privacy, the impact of a privacy

breach, risks associated with reputation,, research motive and public expectations.

- Data controllers and other decision-makers must be fully apprised of their roles and responsibilities,
- Public engagement is an important element of good governance, the attitudes and expectations of the public and other stakeholders should be consulted when constructing a governance approach
- Efficient vetting and training methods are paramount, particularly where the regulatory landscape is confusing and difficult to navigate.

PART 2 GOOD GOVERNANCE IN PRACTICE

Whilst Part 1 was dedicated to outlining our framework of good governance - and notably our proportionate governance framework - Part 2 demonstrates how proportionate governance can be implemented in practice. We offer an overview of how we have actualised a proportionate approach within the SHIP governance framework.

CHAPTER 3 Case Study - Implanting good governance within SHIP

Key question for this chapter:

- How can good governance be implemented in practice?

Key messages from this chapter:

- A good governance framework which stresses proportionality can be implemented within pre-existing organisations and improve considerably upon the regulatory framework
- Such a framework must be clear, transparent and accessible by all individuals at all levels within an organisation and beyond

As mentioned in the introductory section of this paper, the Scottish Health Informatics Programme (SHIP) is a consortium working towards the establishment of the Scottish Health Informatics Platform. The initiative which represents an important step forward for research both within and beyond the medical setting facilitates and oversees the linkage of a vast range of data, thus gaining access to and being jointly responsible for a considerable amount of Scottish population health data.

In order to aid and facilitate discussion about how we have built and implemented a good governance framework within SHIP, we offer a brief overview of the key actors involved with the initiative, their respective roles, responsibilities and relationships, all summarised in the diagrams below.

3.1 SHIP Guiding Principles and Best Practice

The SHIP Guiding Principles and Best Practice[49] offers 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 principles-based approach follows that of the OECD Guidelines[50] in that it identifies areas of governance which are not necessarily found in law and 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. This also takes account of the evidence of public and stakeholder engagement undertaken as part of the SHIP project.

Our Guiding Principles are not intended as replacements to legal rules that already define the different legal responsibilities, limitations and provisions engaged with data sharing. Rather, the guiding principles are companions to legal rules, to assist decision makers where law is silent or decisions requires discretion and judgement. Principles provide a common framework that can assist all relevant parties to identify and balance the key values at stake. Thus:

'Principles' are fundamental starting-points to guide deliberation and action. They reflect the values that underpin the SHIP Infrastructure and its commitment both to promote the public interest and to protect individual interests. Principles are not rules; indeed they sometimes conflict. This is why they are starting points for deliberation or action. However, because of their fundamental importance, it is expected that they are followed where they are

[49] SHIP Guiding Principles and Best Practice can be access at http://www.scot-ship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf

[50] Organisation for Economic Co-operation and Development (OECD) Guidelines for Human Biobanks and Genetic Research Databases (2009) accessible at http://www.oecd.org/dataoecd/41/47/44054609.pdf

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. Together, these principles and best practices are an indication of the standards expected within and upheld by SHIP, and to be adopted by the SHIP infrastructure across Scotland.

In considering its two key principles at stake: (1) promotion of the general public interest and (2) protection of the privacy and other interests of individual citizens, the good governance framework has defined 15 key areas of responsibility and accountability. Appendix 1 contains the SHIP Principles and Best Practice. We have based these around the key issues engaged by secondary uses of health data. These include:

- Public Interest
- Privacy
- Consent
- Anonymisation
- Authorising/advisory bodies
- Governance
- Access
- Trusted Third Parties
- Data Controllers and Data Processors
- Clinical Trials
- Cross Sector Sharing
- Data Sharing Agreements
- Public and Stakeholder Engagement
- Sanctions
- Benefit Sharing

Principles and best practices can be used by:

- Research applicants to determine if their individual and institutional arrangements are sufficiently robust, even before they have submitted applications to SHIP for access

- Data controllers when deciding whether to allow data linkage or inclusion in data in the SHIP model

- Key decision-makers, such as Caldicott Guardians or authorising bodies such as PAC, when deciding whether to permit uses of confidential patient data for research

Here we offer several examples of our Guiding Principles and examples of best practice, which illustrate how the elements of our good governance approach are reflected within them.

PUBLIC INTEREST: The following principle reflects the importance balance to be struck between privacy and the public interest in research:

> *(a) '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.'*

While this principle might seem aspirational, we should not overlook the importance and value of articulating a commitment to these two important social ends. It means in practice that an organisation is duty bound to adopt mechanisms for assessing and balancing the relevant considerations in seeking to due justice to each of these values. Our examples of best practice, then, articulate how this might be done. For example, the best practice example (b) associated with the public interest principles (a) is:

> *(b)'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.'*

RISK-BASED APPROACH: The following examples take from our Guiding Principles and Best Practice document illustrate ways in which a risk-based approach can be operationalised. The articulate both the need in taking a risk-based approach to carrying out assessments and the importance of safe people (who are aware of their responsibilities and the different considerations at stake).

Principles
'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. '

'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.'

Best Practice
'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.'

'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. '

3.2 SHIP Effective and proportionate governance

Proportionality runs throughout our governance framework. It is manifested at different levels and through the various governance mechanisms relied upon. Most notably, the SHIP data access application approvals process (outlined in the section below) adopts a proportionate approach, where the level of scrutiny against which an application is judged corresponds to the level of perceived risks associated with the particular linkage.

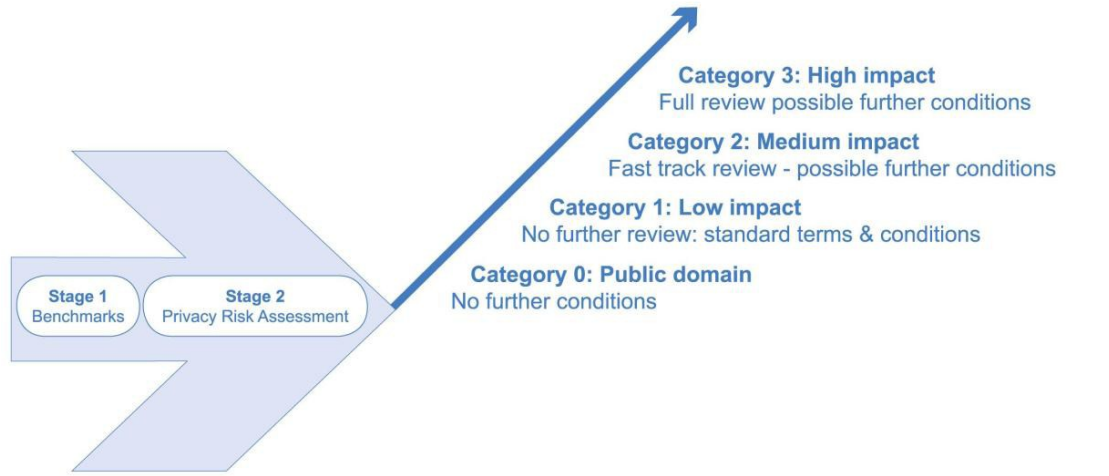
The design of SHIP helps to assure data controller, researchers, research institutions, patients and the public that data linkage within the SHIP context involves **Safe People**, **Safe Data** and a **Safe Environment**. Our vetting and training resources and requirements ensure that individuals accessing valuable data are aware of their responsibilities but also that they are not bogged down by unnecessary formalities or are fearful of misguided sanctions. Rather, researchers will be left confident that they are working within a governance structure designed to facilitate research, rather than to impede it, hopefully harbouring an even more harmonious research culture. Similarly, data controllers and data custodians will rest assured that the data for which they are responsible will only be accessed by suitable individuals in appropriate circumstances, with minimised risk. It is hoped that this will also instil public confidence in health research, and provide reassurance that health data are being put to good use, without compromising privacy concerns.[51]

We have adopted a categorised, risk-based approach to applications, with different categories of risk demanding different levels of scrutiny. This avoids imposing unnecessary burdens upon researchers wishing to access data; it acknowledges the important benefits which health research can bring. However, it also ensures that where risks are involved, appropriate terms and conditions are imposed upon researchers, to ensure that all important considerations, especially privacy concerns, receive due respect and observation.

Our risk-based assessments of the particulars of a data linkage application ensure that the particular risks of individual linkages are more likely to be picked up, whilst at the same time avoiding the temptation to give in to a culture of caution which imposes onerous and unnecessary terms and conditions on researchers and which do not necessarily delivery any higher level of protection to private interests.

[51] For technical details on how SHIP operates, particularly the role of safe havens and the indexer, please consult the SHIP Blueprint, accessible at : http://www.scot-ship.ac.uk/publications

The proportionate and risk-based approach adopted by SHIP towards data access approvals process can be summed up in the following diagram and we explore the different elements and stages represented in the diagram throughout the remainder of this paper.



3.3 A risk-based approach to governance

SHIP has adopted categorisation of data access applications into categories of perceived risk (relating to the elements of risk discussed in Chapter 2). Researchers wishing to access data and data custodians/data controllers are encouraged to carry out a privacy risk assessment, based on the key elements of risk discussed above in Chapter 2 and also to consider the key benchmarks which must be satisfied at all stages of the process, namely: public interest, safe data, safe people, safe environment and relative risks. Researchers can satisfy the criteria of safe people, safe environment and safe data buy taking advantage of SHIP's bespoke technical and governance features, notably: (i) becoming SHIP-accredited researchers (see further below), (ii) operating within the SHIP linkage and safe haven mechanism, and (iii) demonstrating that they operate according to the SHIP Guiding Principles and Best Practices.

It might still be the case, of course, that particular applications to use data raise particular privacy or reputational concerns. The approach allows for an assessment of these. These assessments are then used to map different kinds of applications (based on the level of risk that they represent) onto a range of differentiated governance pathways which deploy different mechanisms to ensure that adequate levels of scrutiny are delivered for each and every application. The system works *both* to increase scrutiny where this is demanded by the prior risk assessment *and* to reduce inappropriate scrutiny where the risk assessment indicates this is warranted. Efficiency gains are returned as a result both with respect to minimising the level of full scrutiny cases and with respect to the 'turnaround' of lower level scrutiny cases.

In this section we outline the different categories of approval adopted by SHIP, and discuss what each entails.

Categorisation

The SHIP online toolkit (discussed at 3.5) will help researchers to anticipate which category their access application is likely to fit under. In turn, this means that the researchers can include the relevant details of relative risks associated with their study, and anticipate the terms and conditions to which an approval might be subject to.

Categorisation is also a manifestation of proportionality, it aids the avoidance of imposing over-burdensome terms and conditions on researchers. For example, in situations where the likelihood of a breach is so small, and the likelihood of subsequent disclosure so small that obliging a researcher to travel all the way to a safe haven facility to carry out the linkage is over burdensome. Categorising such an application as low impact (discussed further below), would remove this burden.

It is appreciated that it is neither possible nor desirable to categorise some applications at a very early stage because risks will ultimately depend on the specifics of each study. Whilst it is envisaged that the majority of applications

will fit under the categories early on, it is acknowledged that there will be a residue of cases that cannot be categorised straight away.

Who will benefit from this approach?

A Research Coordinator will be responsible for advising under which category an application should be made. It is envisaged that with their experience and knowledge, they will be able to discern the appropriate category for consideration. However, as a safeguard, the Data Controller/PAC will have the opportunity to allocate a different category where appropriate.

In what ways in this an example of proportionate governance?

SHIP has taken a 4 levelled approach to categorisation, inspired by the Understanding Society Project Data Access Strategy.[52] The categories are as follows.

Category 0 are data already in the public domain. Applicants should be encouraged to make full use of such data, and these data should be brought to their attention if research questions can be answered without the need to link personal or non-public data.

This categorisation exercise might involve a prospective disclosure control exercise. But, where risks are thought to be minimal or negligible, and in particular where outputs are non-disclosive and non-sensitive, then the application should be assessed as **Category 1**: low impact. No further scrutiny is therefore required and linkage can be performed.

[52] Personal Communication - Economic and Social Research Council, Understanding Society Project, 'Data Access Strategy' Version 19.0. Note this is a draft and not currently available online. It is imperative that there be an approximation of approach within and across sectors to reduce regulatory burden and to help to ensure consistency of decision-making where this is possible.

Category 2 applications are those where issues might be flagged for possible further consideration. These could be sent to PAC in an expedited form and/or dealt with through Chairman's action or via dialogue between then Chair of PAC and the Caldicott Guardian or Data Controllers. Those with higher risks should be labelled as:
Category 3 and subjected to full PAC approval mechanisms.

Appropriate terms and conditions can be associated with different categories of applications. For example, Category 3 might attract additional conditions about security or guarantees of no further linkages. Category 1 should be treated as standard linkages subject to everyday duties of confidentiality and institutional standards.

The following table outlines our proposed categories of application

Category of application	**Type of research falling in to category**	**Appropriate pathway**
Category 0	This category covers 2 types of data: i) Public domain (disclosure controlled); metadata ii) aggregated data (for SHIP-related research); published (SHIP) data;	i) No approval required where information already in public domain ii) Encourage release into public domain of datasets of public interest
Category 1 (Low Impact)	Local researcher; proportionate access; experienced researchers; multiple data controllers within the NHS; non-disclosive/non-sensitive	Data Controller/PAC approval
Category 2 (Medium Impact)	Non-disclosive/sensitive; disclosive/non-sensitive	PAC Triage (Lighter PAC)
Category 3 (High impact)	Disclosive/sensitive	PAC Triage (full PAC)

Whilst proportionality and risk assessment are fundamental to SHIP governance, the structure also relied upon other important elements including guiding

principles, public engagement and vetting and training methods. We discuss these features next.

Identifying appropriate governance pathways

Low impact

Examples of applications that might follow Low Impact research pathway – no need for full review, approval and standard terms and conditions (Fast Track)

- No concerns raised at stages one or two – application is for linkage which is non-disclosive and non-sensitive and safe haven system will be used
- Application is for a particular linkage in keeping with broad purposes already approved between SHIP and trusted researchers for long-term project, e.g. the Scottish Longitudinal Study
- Applications is for a non-contentious extension of a previously approved linkage

Medium Impact

Examples of applications that might follow Medium Impact research pathway – triaged but with option for full review

- Moderate risks or concerns arising from the privacy impact assessment at stage two
- Repeat requests from multiple sector/international/researchers who are able to demonstrate a trusted track record with respect to SHIP
- Application is for a non-sensitive and non-disclosive linkage but safe haven system will not be used

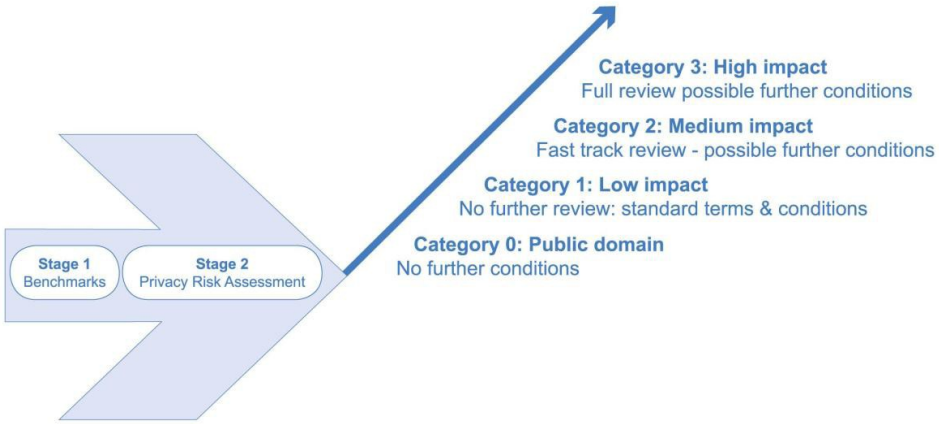
High Impact

Examples of applications that would follow the High Impact research pathway – requiring full review

- Failure to satisfy any one of the criteria for assessment at stage one (e.g. – questions over the public interest in the research, safe people, safe systems or safe environments, or wider risks such as reputation of the data controller)
- Concerns arising from the privacy impact assessment at stage two (e.g. – very sensitive data; serious risks of disclosiveness)
- Multiple sector or international linkage being requested for the first time.

In all cases, appropriate terms and conditions for sharing and linkage will reflect the nature of the governance pathway followed by any given application.

Once more, we draw your attention to the diagram below, which represents the SHIP approvals process:



We have included both stage 1 and stage 2 prior to our categorisation of pathways. Arguably, these function, first, to allow the benchmark to identify any early concerns which – if present – automatically mean that full review (category 3) is required. Only if this is not the case do we then perform a privacy risk assessment which helps to discern the granularity of the application in terms of its risks.

3.4 SHIP Roles and Responsibilities of Data Controller

Researchers are not the only actors challenged by the complex legislative provisions. Indeed data controllers, who are identified in law as the individual(s) responsible for discharging data protection obligations often find it difficult to discern what their roles and responsibilities are at different stages of research.

The confusion is exacerbated where data are transferred between individuals or organisations and datasets are linked. Data Controllers (either alone or jointly or in common with other persons) determine the purposes for which and the manner in which any personal data are, or are to be, processed. Further, Data Processors, defined as any person '…other than an employee of the data controller who processes data on behalf of the data controller'[53] also have responsibilities for datasets.

Good governance recognises the importance in individuals and organisations having full awareness of their responsibilities and how and when these are engaged. An important point, which is often forgotten, is that the European Data Protection Directive was drafted not only in order to ensure data is adequately safeguarded from related risks, but also to facilitate data sharing, particularly for purposes in the public interest. It is not only important that Data Controllers know when they cannot or should not share data, but also when they can and should do so. The SHIP Online Toolkit, which is one of the key components of the Researcher Training Package, is designed to help data controllers and data processors to understand their responsibilities as well as acting as a tool to train researchers. [54]

3.5 SHIP Researcher Training

Despite the strong benefits that a proportionate approach to governance can bring, we acknowledge that proportionality on its own is not enough to ensure a smooth running and effective framework. Proportionate governance, and the promise it holds can be easily lost on a lack of sound vetting and training methods. It is essential that all actors involved understand the different

[53] Data Protection Act 1998

[54] SHIP 'Functions, Roles and Responsibilities of Data Controllers', see http://www.scotship.ac.uk/sites/default/files/Reports/Appendix_6.pdf

considerations at stake, the responsibilities they hold, the points at which they hold them, the standards to which their conduct will be held and the repercussions when they fail to meet these standards.

There are claims within the literature (and our own SHIP research) that indicate that researchers in particular lack confidence when it comes to discerning what are their responsibilities.[55] Similarly, the current legislative and regulatory landscape does not always make it clear when different actors are responsible for data and when this shifts/is jointly held with other actors.

In response to this clear need for proportionate and effective vetting and training methods SHIP is currently developing a training strategy for SHIP users, and those involved in secondary data uses more generally.

This strategy includes 3 main elements - a researcher toolkit, learning module and researcher passport.

The toolkit is an online resource which provides users with an overview of the different ethical and legal considerations involving secondary uses of health data. It includes a clear and concise overview of key responsibilities and working examples of how to fulfil these responsibilities. The toolkit outlines how SHIP operates, and how it can support data controllers and researchers. Although the toolkit is primarily designed for researchers and data controllers, it will be accessible to a range of different actors, which, it is hoped, will help to harmonise practices across the health research community.

The learning module is an expanded version of the toolkit, and it offers a more in-depth overview of the ethical and legal issues engaged with health research involving secondary data. Thus, users will be equipped with the knowledge and skills needed to understand the responsibilities and opportunities open to them, as well as what is expected of them and what they can expect from data custodians and authorising bodies. The module consists of assessments at the

[55] Publication forthcoming - authored by Cunningham-Burley S, Laurie G, Pagliari C, Aitken M, Sethi N

end of each topic, and a compulsory assessment which users must complete and pass at the end in order to gain approved researcher status.

Approved researcher status will permit individuals to access the vast and rich datasets that will be brought under the auspices of SHIP, it will also help to speed up the approvals process when vetting data access applicants, as approved status signifies that the individual understands their responsibilities and how to navigate themselves around their responsibilities in accordance with the demands of the good governance framework.

In addition to the SHIP Toolkit and Module, the programme has introduced the role of a Research Coordinator (RC). The RC will be responsible for overseeing data access applications, and streamlining the process, acting as a liaison where needed between researchers and data controllers as well as offering advice. The RC role will be fulfilled only by individuals with the requisite level of experience in navigating the landscape. They will assist users of SHIP to navigate the system, providing guidance on each step, and acting as gatekeeper to training and accreditation services. They will be responsible for scrutinising data requests for compliance with access requirements, data access arrangements and the facilitation of dissemination of research outputs, all in accordance with SHIP's good governance framework.

3.6 Conclusion

This chapter has demonstrated how a good governance framework can be implemented within the health research setting drawing on the SHIP model.

Key messages from this chapter include:

- Key features of the SHIP governance model embody proportionate and risk-based approaches.
- The SHIP Guiding Principles and Best Practice represent an expression of the values that should underpin all levels of decision-making.

- Safe, effective and proportionate governance includes: (1) proportionality as an overarching theme and (2) an explicit risk-based approach to governance, which can be operationalised by adopting authorisation as a governance mechanism.
- The SHIP data access application approvals process adopts a proportionate approach, where the level of scrutiny against which an application is judged corresponds to the level of perceived risks associated with the particular linkage.
- The approvals process allows researchers to anticipate the terms and conditions they might have to satisfy, and it can reassure data custodians that sufficient benchmarks are being met prior to data sharing
- Good governance recognises the importance in individuals having full awareness of their responsibilities and how and when these are engaged
- An on-line toolkit and learning module can prove an effective resource for the research community, particularly in terms of offering transparency regarding the different roles, responsibilities and expectations within the governance landscape, but also in instilling confidence and encouraging a culture of collaboration as opposed to caution.

CHAPTER 4 Conclusions

This paper has laid out the key components of our good governance framework and the SHIP case study as a demonstration of how the elements of the framework can be operationalised.

Summary of key messages

- Through our collaborative work with SHIP, we have adopted an **iterative, multidisciplinary and discursive approach** in developing our good governance framework.

- Our **good governance framework** consists of 4 key components: (1) Guiding Principles and Best Practice; (2) Safe, effective and proportionate governance; (3) Roles and Responsibilities of Data Controllers and (4) Researcher Training

- **Guiding principles and instances of best practice** are an effective way of articulating the values and principles which should be respected throughout an organisation, as well as how these can be implemented in practice.

- Key elements of **safe, effective and proportionate governance** include: proportionality; a risk-based approach; guiding principles and best practice, public engagement and vetting and training methods.

- **Proportionality** should feature as a dominant over-arching theme of good governance; it involves allocating precautionary measures and disciplinary mechanisms which appropriately reflect the perceived risks or damages of actual breaches**.**

- **Proportionate governance** is a multi-faceted enterprise, including not only risk/benefit analysis, but also considerations of reputational risk & implications for public trust, the assessment of the relative merits of preferring certain governance mechanisms and the allocation of appropriate governance pathways drawing on a range of governance tools as suitable for any given research application

- A **risk-based approach** provides the most appropriate approach to proportionate governance. It involves consideration of key risk-related benchmarks which include: the public interest, safe data, safe people, safe environment, consideration of relevant risks and risk assessment**.** Such an approach strikes appropriate balance between promoting important values and facilitating research in the public interest

- Authorisation is an effective governance mechanism for operationalising a proportionate, risk-based approach to governance and can be used alone or in combination with other, more traditional, approach such as consent or anonymisation. Proportionate governance allows a more bespoke and effective deployment of these mechanisms than currently exists in many contexts.

- A good governance framework which stresses proportionality can be implemented within pre-existing organisations and improve upon the regulatory framework considerably**;** such a framework must be **clear, transparent and accessible** by all individuals at all levels within an organisation, as embodied by the SHIP governance model.

- **Categorisation of applications** to approval pathways enables a proportionate approach to governance, where the level of scrutiny

against which an application is judged corresponds to the level of perceived risks associated with the particular linkage.

- The approvals process allows researchers to **anticipate** the terms and conditions they might have to satisfy, and it can **reassure data custodians** that sufficient benchmarks are being met prior to data sharing

- Good governance promotes the importance in individuals having full awareness of their responsibilities and how and when these are engaged

- Research training should consists of **effective resources** for the research community, particularly in terms of offering transparency regarding the different roles, responsibilities and expectations within the governance landscape, but also in instilling confidence and encouraging a culture of collaboration as opposed to caution.

- Due regard must be given to, and an appropriate accommodation arrived at, as between the various **ethical and legal considerations at stake** – different governance mechanisms can be deployed **alone or in combination** to achieve this, and their relative merits and limits must be understood accordingly.

Acknowledgements

We would like to thank all those who have given up their time to participate in and facilitate the development of our good governance framework, particularly those involved in the Scottish Health Informatics Programme, too numerous to mention as part of such a diverse collaborative team. In particular, we would like to thank Sarah Sutherland and Emily Postan for their ongoing efforts in developing the SHIP training programme. All errors are the responsibility of the authors.

References

Academy of Medical Sciences Response to Data Sharing Review – see www.acmedsci.ac.uk/download.php?file=/images/publication/...pdf

Academy of Medical Sciences, (2006) 'Personal data for public good: using health information in medical research'. See http://www.acmedsci.ac.uk/p48prid5.html

Al-Shahi R, Warlow C (2000) Using patient-identifiable data for observational research and audit. BMJ 2000;321:1031-1032

Banff Executive Leadership Inc (2004) 'Improving Governance Performance: Rules-Based vs Principles-based Performance' in Leadership Acumen Issue 16 Jan/Feb 2004

Beauchamp T and Childress J (2008) 'Principles of Biomedical Ethics' Sixth Edition, Oxford University Press

Black J, 'Forms and Paradoxes of Principle Based Regulation' LSE Law, Society and Economics Working Papers 13/2008 accessible at: http://eprints.lse.ac.uk/23103/1/WPS2008-13.pdf

Black, J, 'The "Principles" Paradox' (March 1, 2008), Duke Law School Legal Studies Paper No. 205 Available at SSRN: http://ssrn.com/abstract=1121454

Ciancardo J, (2009) 'The Principle of Proportionality : its Dimensions and Limits'

Clark, S and A Weale. 2011. "Information Governance in Health: An Analysis of the Social Values Involved in Data Linkage Studies." The Nuffield Trust Available at: http://www.nuffieldtrust.org.uk/sites/files/nuffield/information_governance_in_health_-_research_report-_aug11.pdf

Commissioner McCreevy (2007), 'Capital Market Place' in Wall Street Journal 5th March 2007, available at http://www.eurunion.org/newsweb/EUInMedia/cmcWSJoped030507.htm

Confidentiality & Security Advisory Group for Scotland (2001) 'Protecting Patient Confidentiality: A consultation paper, Seeking Consent' http://www.csags.scot.nhs.uk/ppc/ppc.pdf.

Data Protection Act (1998)

Department of Health, Research Governance Framework for Health and Social Care: Second Edition (2005) See http://www.dh.gov.uk/en/Publications

FSA (2007) 'Principles Based Regulation: Focusing on the Outcomes that Matter'

Gunn T, 'Deconstructing Proportionality in Limitations Analysis' in Emory International Law Review, Vol 19 (2005) 465 - 498

Harbo T, (2010) 'The Function of the Proportionality Principle in EU Law' in European Law Journal Volume 16, Issue 2, pages 158–185

HaynesCL, Cook GA and Jones MA (2007) 'Legal and ethical considerations in processing patient-identifiable data without patient consent: lessons learnt from developing a disease register', *Journal of Medical Ethics* 33, 302–7.

International Monetary Fund (2005) 'The IMF's Approach to Promoting Good Governance and Combating Corruption — A Guide'see http://www.imf.org/external/np/gov/guide/eng/index.htm

Iverson A et al (2006) 'Consent, Confidentiality and the Data Protection Act' in British Medical Journal 332:165

Laurie G and Sethi N, 'Information Governance of Use of Health-Related Data in Medical Research in Scotland: Current Practices and Future Scenarios' (2011) University of Edinburgh Law Working Paper No. 2011/26 Accessible at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1946258

National Health Service Act 2006

NHS NSS Caldicott Guardians, see : http://www.nhsnss.org/pages/corporate/caldicott_guardians.php

NHS NSS Privacy Advisory Committee for Scotland, 'Guiding Principles and Policy for Decision-Making and Advice' accessible at http://www.isdscotland.org/isd/servlet/FileBuffer?namedFile=PAC-Guidance-on-decision-making.pdf&pContentDispositionType=inline

Nicolson D and Wyatt J, (2010) 'A Systematic Review Examining Evidence Relating to the Reuse of People's Medical Records for Research Purposes'

Organisation for Economic Co-operation and Development (OECD) Guidelines for Human Biobanks and Genetic Research Databases (2009) accessible at http://www.oecd.org/dataoecd/41/47/44054609.pdf

Paul Ohm 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' 57 UCLA Law Review 1701 (2010)

Peto J, Fletcher O and Gilham C (2004) 'Data protection, informed consent and research: medical research suffers because of pointless obstacles' (editorial), *British Medical Journal* 328, 1029–30

Proposal for a new Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the

free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final accessible at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Seligman C, Syme G, Gilchrist R (1994), 'The Role of Values and Ethical Principles in Judgments of Environmental Dilemmas ' in Journal of Social Issues Volume 50, Issue 3, pages 105–119

SHIP 'Functions, Roles and Responsibilities of Data Controllers', see http://www.scotship.ac.uk/sites/default/files/Reports/Appendix_6.pdf

SHIP Guiding Principles and Best Practice can be access at http://www.scot-ship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf

SHIP: A Blueprint for Health Records Research in Scotland: Draft for consultation (2011) see http://www.scot-ship.ac.uk/sites/default/files/Reports/SHIP_BLUEPRINT_DOCUMENT_draft_for_consultation_081211.pdf

Siddiqi S et al (2009)'Framework for assessing governance of the health system in developing countries: Gateway to good governance' in Heatlh Policy Volume 90, Issue 1 , Pages 13-25, statistics/Publications/PublicationsPolicyAndGuidance/DH_4108962

Strobl J, Cave E and Walley T (2000) 'Data protection legislation: interpretation and barriers to research'; *British Medical Journal* 321, 890–2

The Independent Commission on Good Governance in Public Service (2004) 'The Good Governance Standard for Public Services'. See http://www.cipfa.org.uk/pt/download/governance_standard.pdf

The Rt. Hon. Lord Justice Stanley Burnton, 'Doctors, Patients and the Human Rights Act' Medico-Legal Journal (2011) Vol. 79 Part 4, 115–128.

The Scottish Government,' NHSScotland Caldicott Guardians: Principles into Practice' see http://www.scotland.gov.uk/Publications/2011/01/31115153/1

United Nations Economic and Social Commission for Asia and the Pacific 'What is Good Governance?' http://www.unescap.org/pdd/prs/projectactivities/ongoing/gg/governance.asp

Van Gerven, W, The Effect of Proportionality on the Actions of Member States of the European Community: National Viewpoints from Continental Europe, in The Principle of Proportionality in the Laws of Europe (Evelyn Ellis ed., 1999

APPENDICES

Appendix 1
SHIP: Guiding Principles and Best Practices

A document of the SHIP Information Governance Working Group (October 2010)

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.

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 data storage facility that provides secure access to data for approved researchers, carries out SDC on outputs and may also contain a safe haven for secure local and/or remote access.
(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.[56]

- 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.

3. Consent

Principles

[56] 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

- 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 a recognised 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 in function of 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[57]

- 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[58])

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, authorisation 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)

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

[58] 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

- 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, approval from an independent oversight body/research ethics committee should be obtained.

- 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.[59]

- 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.

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.[60]

- All stakeholders and research users should undertake the SHIP training online module on *Information Governance: Rights and Responsibilities*.[61]
- 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

[59] The Nolan Principles are elaborated in Appendix X.
[60] This report is available from the SHIP Website accessible at …
[61] To be developed in due course via the Edinburgh Law School eSCRIPT distance learning platform.

authorising and/or advisory body. Those involved with this oversight should have the relevant expertise to carry out such responsibilities.

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.[62]

- 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).

[62] 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.[63] Ideally, all staff, data recipients and research users should undertake the SHIP training online module on *Information Governance: Rights and Responsibilities*.[64]

- 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.

[63] 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.

[64] To be developed in due course via the Edinburgh Law School eSCRIPT distance learning platform.

- 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.[65]

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.[66]

- 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.[67]

- 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.

10. Clinical Trials

Principles

[65] 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

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

[67] 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.

- 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 should 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.

Appendix 2

Functions, Roles and Responsibilities of Data Controllers

Background

The UK Data Protection Act 1998 (DPA) came into force on 1 March 2000 and is the UK enactment of the European Data Protection Directive 95/46/EC.

At present the UK Government is gathering evidence on Data Protection practice and experience under the DPA in anticipation of negotiations for a new Data Protection Directive in 2011.

In the meantime all UK individuals and organisations must ensure that their use and disclosure of personal data complies with the requirements of the DPA.

Key Concepts

Identifying the Data Controller

The DPA confers the responsibility and liability for compliance with the requirements of the DPA on the Data Controller. Identifying the Data Controller(s) in relation to a set of personal data and its processing operations is therefore key to ensuring that data protection obligations are known and adhered to. It is sometimes challenging to identify the Data Controller where a number of actors and processing operations are involved.

The opinion of the Article 29 Data Protection Working Party[68] published in 2010[69] recognised the challenge in this area. The Working Party made some unambiguous observations:

In identifying a Data Controller, identifying who sets the purposes of the processing is the paramount consideration;
The actors involved must have the legal and factual capacity to fulfil their role i.e. a Data Controller is not a Data Controller unless in facts and law they have the capacity to set the purposes for the processing of the personal data;
A pluralistic situation, with a number of Data Controllers, including with different degrees of responsibility and liability, is both possible and acceptable.

[68] The Article 29 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.

[69] Opinion 1/2010 on the concepts of 'controller' and 'processor' , 00264/10/EN, WP 169, adopted 16 February 2010

Key messages:
It is essential to be clear as to who is acting as a data controller with respect to any given data set which involves the processing of personal data
It is possible that one or more parties can act in the capacity as a data controller and will accordingly be held jointly liable
It is possible to agree between parties who will act as a data controller with respect to a given dataset and/or to agree difference levels of responsibility and liability

Data Controllers and Data Processors
The Data Controller is defined as the person or persons who determines the 'purposes for which and the manner in which personal data are to be processed'.

The Data Processor is defined as any person '…other than an employee of the data controller who processes data on behalf of the data controller'.

Data Controllers and Data Processors are typically organisations, authorities or businesses e.g. the Data Controller of the personal data used across NHS hospitals in the Lothians area is Lothian NHS Board.

An important feature of the Data Controller/ Data Processor relationship is that the Data Controller retains liability under the DPA for all processing of personal data undertaken by the Data Processor on their behalf. There is a legal requirement that a written contract between the Data Controller and Data Processor governs processing undertaken by a Data Processor on behalf of a Data Controller.

Data Controllers may only disclose personal data in accordance with their Register entry in the Information Commissioner's Register of Data Controllers, and the Data Protection Principles set out in Schedule 1 of the DPA. Whilst the Data Controller is legally required to ensure that all disclosures of personal data meet these requirements, they do not retain these obligations after the data are disclosed. These obligations essentially flow to their recipient, who then becomes the Data Controller and liable for their use and disclosure in accordance with DPA.

Key messages:
Data controllers retain legal liability with respect to processing of data and the activities of data processors who work on their behalf until such time as data are disclosed
It is imperative to be clear with respective parties as to the capacity in which they are entering a relationship and also the point at which the responsibilities of data controller(s) will pass (if at all).

Processing

The DPA defines 'processing' widely so as to encompass virtually anything that might be done with personal data (e.g. obtaining, storage, the act of anonymisation, use, disclosure, destruction) throughout its lifecycle.

Appendix 3
SHIP Researcher Training Module

The SHIP Researcher Training Module comprises of 2 key components:

(1) Online Toolkit

The SHIP Information Governance Toolkit is designed to be an easily accessible online facility which assists in the navigation and understanding of the often complex legal concepts and legal framework which govern the use of data. The Toolkit is primarily aimed at research using electronic patient records, however the guidance provided is applicable more generally to all uses of information for research and other purposes. It is principally designed to be used by researchers and data custodians seeking to use the SHIP framework, however it is envisaged that it will be a useful resource for those involved in healthcare research more generally.

Key modules/content

The Toolkit is divided into six main sections as follows:

1. Legal Concepts
   This section of the Toolkit contains information pages on the key legal concepts of Autonomy and Consent, Anonymisation, Confidentiality and the Public Interest. Within each information page is a 'Takeaway Toolkit' which users can download for quick reference purposes.

2. Legal Framework
   Here practical information is given on how to navigate the legal framework governing information. Guidance is given on the Data Protection Act 1998, the Human Rights Act 1998, the common law of confidentiality and the Freedom of Information Acts. The information pages in these sections seek to explain what the law is and what specific obligations researcher and data custodians have under this framework. Within each page can be found a 'Takeaway Toolkit' which provides a brief outline of the key points arising from each source of law.

3. Roles & Responsibilities
   This section provides users with guidance on the responsibilities they have either as a researcher or a data custodian. It also seeks to provide clarification on the roles of the various authorising and advisory bodies who are involved in governing the use of information.

4. Route Maps
   This section features interactive route-maps and forms the main part of the Toolkit. The route-maps have been designed to take users through the SHIP processes and to present the legal concepts and legal framework in a practical and accessible format. There are four route-maps:

1. *Researchers: making an application to access data through SHIP*
   This route-map is designed to take researchers through the practical steps that they will need to make when making a data access application through SHIP. In particular is focuses on how researchers should assess the privacy risks associated with their data access application.

2. *Researchers: navigating consent issues*
   Here researchers are guided through the legal, ethical and practical considerations which they may face when they seek consent to access data for their research purposes.

3. *Researchers: managing data security during life of research project*
   In this route-map researchers are taken through the steps that they must take in order to comply with the legal requirements and ensure data security through the life of their research project. Guidance is given on the security considerations both during the research project and after the research project has been completed.

4. *Data Custodians: assessing requests for data access through SHIP*
   This route-map is intended to be used by data custodians. It explains how the SHIP framework can benefit data custodians and takes them through the SHIP process that data will go through before it is released to researchers.

5. Scenarios
   Here guidance is given to users as to how to apply the knowledge they have acquired in practical scenarios. Particular focus is on how to determine whether it is appropriate to use a SHIP Safe Haven or whether there can be direct data transfer, and on the type of applications which will fall into the SHIP privacy risk categories.

6. Links & Resources
   In this section of the Toolkit, users can find links to both external sources of information, as well as to the guidance documents provided elsewhere in the Toolkit, such as the Takeaway Toolkits.

(2) Distance Learning Module

This SHIP: Information Governance distance learning module has been developed alongside the SHIP Toolkit as an educational resource for researchers. The module seeks to advance the understanding of information governance gained through use of the Toolkit, as well as to help researchers develop core skills and an increased awareness of the importance of information governance. Completion of the module is a prerequisite for any researcher who seeks to access data through the SHIP infrastructure.

Key Modules/content

The module is divided into six sessions as follows:

1. Legal Concepts
   This session is provided as an overview of the key legal and ethical concepts which are relevant to the legal framework governing the use of information. It covers largely the same material as the corresponding section of the SHIP Toolkit, but provides more detailed information.

2. Legal Framework
   This session is provided as an overview of the legal system in general and of the specific legal framework which governs the use of information. Again it covers very much the same material as the SHIP Toolkit, but more detailed information is given.

3. 'Safe Projects'
   Here the importance of good information governance is discussed, and information is given on the SHIP approach to information governance. Guidance is also given on the importance of privacy risk assessments and how to complete them.

4. 'Safe Data'
   In this session the legal framework governing the use of data is considered in more detail, with particular attention being given to the Data Protection Act 1998. Specifically, the session will examine the different ways in which access to personal data can be obtained and how personal data can be lawfully processed.

5. 'Safe Settings'
   This session examines data security. It looks at how data can be kept secure both during and after a research project and explores both the legal and practical considerations. This session seeks to build on the information given in the SHIP Toolkit.

6. 'Safe Outputs'
   The focus of this session is to discuss how to ensure that the outputs of a research project and safe and secure, and in particular guidance is given on the process of statistical disclosure control.

At relevant points throughout the module, researcher will be able to complete scenario-based self-assessment quizzes. The purpose of these is to allow researcher to test their own practical understanding of the course material.

At the end of each session researchers will have to complete an assessed multiple-choice quiz. These quizzes are simply designed to ensure that the researcher has understood the information provided in the session. Although the researcher needs to obtain a score of 100% in order to pass the assessment, they will have an unlimited number of attempts at the quiz. The number of attempts takes will however be recorded in order that action can be taken should any problems become evident.