Information Governance of Use of Health-Related Data in Medical Research in Scotland

University of Edinburgh
School of Law

Working Paper Series

No 2011/26

Information Governance of Use of Health-Related Data in Medical Research in Scotland: Current Practices and Future Scenarios

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

Abstract

This paper has been prepared as part of the governance work stream of the Scottish Health Informatics Programme (SHIP). It is intended as a platform for discussion and further elaboration with colleagues and those interested in issues surrounding the governance of secondary uses of health data for research. The main aims of the paper are two-fold. First, to offer an ethical, legal and social account of the current regulatory framework governing the use of person identifiable information (PII) for medical research in Scotland. It does so by both mapping out the legislation and key actors involved in governance, as well as illustrating how the framework is perceived to work in practice. A second aim of the report is to suggest a template to be used in the assessment of good governance. This template can be used both to evaluate current practices and to test any proposals for change in approaches to governance in Scotland and elsewhere with respect to uses of patient data for research purposes. It is anticipated that this template will be developed and refined with input from SHIP colleagues (particularly those at Information and Statistics Division (ISD) of NHS Scotland and those involved in the SHIP Systematic Review) as well as other stakeholders. This is the first in a series of papers in the governance stream of the SHIP programme, funded by the Wellcome Trust. Future papers will address the design challenges of a new system of information governance for health-related medical research in Scotland.

Keywords

Information governance : governance: personal data; patient identifiable information; secondary uses of data; research; SHIP; health informatics; regulatory landscape

TABLE OF CONTENTS

Part 1 – Introduction: Setting the scene, social and ethical considerations, and objectives of the stream

Chapter 1 Introduction

1.1 The aims of the paper

This paper has been prepared as part of the governance work stream[1] of the Scottish Health Informatics Programme (SHIP). It is intended as a platform for discussion and further elaboration with colleagues and those interested in issues surrounding the governance of secondary uses of health data for research. The main aims of the paper are two-fold. First, to offer an ethical, legal and social account of the current regulatory framework governing the use of person identifiable information (PII) for medical research in Scotland. It does so by both mapping out the legislation and key actors involved in governance, as well as illustrating how the framework is perceived to work in practice.

A second aim of the report is to suggest a template to be used in the assessment of *good governance*. This template can be used both to evaluate current practices and to test any proposals for change in approaches to governance in Scotland and elsewhere with respect to uses of patient data for research purposes. It is anticipated that this template will be developed and refined with input from SHIP colleagues (particularly those at Information and Statistics Division (ISD) of NHS Scotland and those involved in the SHIP Systematic Review) as well as other stakeholders. This is the first in a series of papers in the governance stream of the SHIP programme, funded by the Wellcome Trust. Future papers will address the design challenges of a new system of information governance for health-related medical research in Scotland.

[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.
Nayha Sethi is a Research Fellow and PhD Candidate at the AHRC/SCRIPT Centre, School of Law, University of Edinburgh.

Definitions

From the outset, we should clarify that when referring to 'medical research' this should be understood to include a wide variety of forms of investigation, including research done for medical purposes as well as research done using medically-related or health-related data. Accordingly, any governance system that is designed to encourage such research must be sufficiently flexible to accommodate a range of different kinds of investigation or applications. It is another matter whether distinct kinds of applications are successful, and this will fall to be considered on a case by case basis. In all cases the appropriate protection of patient privacy will be of paramount concern.

When we refer to PII (person identifiable information), we are concerned with the definition of personal data contained in the EU Data Protection Directive, viz: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, social or cultural identity'.[2]

When it comes to the purposes for which data are collected and used, it should be noted that indistinct boundaries exist between research and audit. It is argued in some quarters that this should impact on the governance regimes that apply. Furthermore, and more recently, there has been a shift in the purpose and manner in which data are controlled in collections, namely from specific disease collections to 'research resource' i.e. whereas database linkage was previously aimed at specific disease study, now, databases exist which are vast resources with which to perform linkages between disease registers or other types of database e.g. link between diabetes and liver disease.[3] It should also be noted that much of the research relevant to our discussion does not involve linkage; notwithstanding, most of the issues remain where we are accessing existing core datasets even without any linkage.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Article 2(a) (hereafter referred to as the Data Protection Directive 95/46/EC)

[3] The linkage of datasets and causal or statistical linkages between risk factors and clinical outcome should be differentiated.

We repeatedly refer to optimal governance throughout the paper. It is a term which we feel reflects the standard of health information governance towards which we should strive. We partially base this standard on key elements of optimal governance proposed by Sir Alan Langlands. These include '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] In addition to these elements, it is a given that respect for the legal and ethical principles outlined in this paper are integral to achieving optimal governance. Moving beyond these considerations, we propose that a system of optimal governance must also be a system of *proportionate governance*, that is, one which establishes and operates mechanisms that, in its procedures and invasiveness, is relative to the risks and benefits which data linkage can bring.

As the term suggests, proportionate governance reflects a philosophy towards governance which emphasises proportionality; the level of governance which a process, procedure or individual is subject to should correspond to the level of potential risk involved in their actions. In other words, the governance standards which have to be met should not be disproportionate to the activity being pursued. This approach of proportionate governance was partially inspired by the 2011 AMS Report 'A new pathway for the regulation and governance of health research'[5] which stressed the need for proportionate governance, as a reaction to the over burdensome landscape governing data reuse for research.

A final point to note concerns the nature and location of datasets themselves. Whilst for the purposes of SHIP, we are primarily discussing the linkage of NHS ISD datasets (either with other NHS data or data from non-NHS sources), it must be recognised that even in this context data are shared and linked with a wide range of entities, both health

[4] 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

[5] Academy of Medical Sciences ''A new pathway for the regulation and governance of health research' Jan (2011).

and non-health related, and involving both academic/public and private/commercial institutions. In terms of governance, then, any recommendations offered here should be taken to be applicable to (health) data used in a wide range of contexts, whether this concerns NHS (health) data or not. Other terms, such as *consent* and *anonymisation* are defined in the relevant sections of this report

1.2 Sources

An array of sources has been used in the writing of this report. First, primary and secondary key legislation was consulted as well as relevant case law. Further, the roles of actors involved in governance in this area were documented, including data controllers (notably NHS ISD), Caldicott Guardians and the Information Commissioner. Good practice guidelines from professional associations such as the General Medical Council and recommendations emerging from consultation reports were also considered.[6] Further information was gathered from secondary academic literature such as journal articles. Finally, input was also sought from those engaged with using the governance framework on a day to day basis, individuals such as data controllers and medical researchers. We are grateful in particular to the following individuals who provided useful input on earlier versions of this report: Patricia Ruddy, Anthea Springbett, Andrew Morris, Violet Warwick, Ian Ford, Yvonne Hopf, Sarah Clark, Albert Weale, Donald Nicolson and D'Arcy Holman.

1.3 Legal Background

Given the parmountcy of privacy protection in this report it is appropriate to begin by considering relevant international and domestic legal instruments. The EU Data Protection Directive from 1995 led to the adoption by the United Kingdom of the Data Protection Act 1998, which introduced its Eight Principles, requiring the UK to reassess and regulate the manner in which data are processed (including data gathering, storage and disclosure). Further, with the introduction of the Human Rights Act 1998, the importance of the individual's right to respect for private life, and to determine with whom and how s/he shares personal information, was highlighted.

[6] Kaye J and Gibbons S, 'Mapping the regulatory space for genetic databases and biobanks in England and Wales', Medical Law International, 2008, Vol 9, pp111-130 offered a helpful approach for scoping out the current legislative framework and we have borrowed this in the present report.

It is important to note, however, that the law does not give privacy an absolute value. Due consideration must also be given to the rights and interests of others as well as the public interest in processing PII. Thus a balance is continually sought between respecting an individual's privacy, including personal information relating to their health in the context of PII in medical research, and the potential benefits to the population through disclosure of their data for medical research and other purposes e.g. audits. In particular, it is widely accepted that the potential for benefiting the population's health can be promoted considerably through linking different sets of data together, thus providing a richer set of data with which to conduct research.

From a privacy perspective, however, one obstacle stands in the way of data linkage, that is, where two or more data sets are linked, it may become possible to identify an individual from the data, thus potentially endangering their right to privacy.[7] One commonly-adopted solution to the management of this risk has been to anonymise or pseudonymise the data, that is, to modify the data so that personal identifiers are removed and/or encrypted thus lessening the possibility of identity disclosure. Appropriately anonymised data are not caught by the provisions of the data protection law. Unfortunately, an unlooked-for consequence of such processes might be that the richness and thus the potential benefits from the data linkage may be lost this way.

An alternative to anonymisation is the practice of gaining the data subject's consent to use their PII for research. This is thought to legitimate processing in ethical terms since it is a measure of respect for the person and his/her wishes; it is also a commonly-viewed device to ensure compliance with the law. However, as we will learn later, obtaining consent is no easy feat. Further, it should be noted that obtaining consent does not remove other responsibilities owed concerning appropriate processing of PII under data protection law. Indeed, while the obtaining of consent might be viewed as a measure of best practice, it is neither necessary nor sufficient in terms of strict law.

Authorisation also plays a key role in the use of PII for medical research. This is often given by an appropriately-constituted independent body when consent cannot

[7] We accept that mere identifiability does not necessarily endanger an individual's privacy save that identifiability is the trigger threshold for protection of personal data under the Data Protection Directive.

practicably be obtained and if researchers wish to use PII in an identifiable form. Indeed, even when data are to be used in an anonymised form, approval must often be sought from an authorising body. Such authorising bodies can operate with or without a clear legal basis. An example of a legal body operating in this way is the Ethics and Confidentiality Committee (see further below p38). Scotland has no such body at present. The closest example is the Privacy Advisory Committee which merely provides advice to NHS ISD and National Records of Scotland on data use and does so on a non-statutory footing[8].

A further obstacle to data use and sharing concerns the ethical, legal and professional obligation of confidentiality. This is a primary concern, particularly for doctors and other health care professionals who may deem GMC Confidentiality guidance to be strongly compelling and militating against disclosure. NHS Staff also focus on the common law duty of confidentiality in their day to day business and are required to sign confidentiality agreements with respect to the data they encounter and handle in their working practices. Concerns for confidentiality, while well-based, can give rise to a culture of caution when it comes to the prospect of data use and sharing. Once again, an obligation of confidentiality is not necessarily absolute in law but the precise parameters of legitimate action can be difficult to identify.

Thus a solution must be sought, one which respects the important and often competing considerations of respect for privacy and the public interest, as well as respecting the law and being practicable in reality.

1.4 Why the landscape is so complex

The governance of PII for medical research is by no means lacking in flaws; in fact, the wider governance framework concerning data protection in general has received considerable criticism.[9] The confusion ranges from questions as to which legislation is

[8] PAC operates under the auspices of National Services Scotland. More information can be found here: http://www.nhsnss.org/pages/corporate/privacy_advisory_committee.php

[9] An example of just how many pieces of legislation are potentially involved is offered in the House of Lords Report on Genomic Medicine (July 2009). Andrew Morris commented on the regulation of genetic research in the UK -"The Department of Health guidance suggests that this domain is affected by 43 relevant pieces of legislation. There were 12 sets of relevant standards and eight professional codes of conduct. What this has bred is a culture of caution, confusion, uncertainty and inconsistency" (para 6.15) House of Lords, Science and

engaged and how, to questions of the correct procedures for requesting access to PII, to what extent data may be used, by whom, for what purposes and under which conditions. At the time of writing, the European Data Protection Directive[10] is under review, partly in response to the need for more clarification on its provisions.[11]

Problems are heightened in the PII context by the existence of authorising or advisory bodies such as research ethics committees (RECs) or the Privacy Advisory Committee (PAC) sometimes lacking formal authority or adequate powers, yet which are charged none the less with regulating or overseeing the use of PII.

The many different actors, vague and sometimes conflicting rules/guidance and difficulty reconciling privacy and public interest considerations all add to the labyrinthine structure of the law and considerable confusion in practice. The distribution of data controller and data processor roles (see page 43) across the NHS - which is neither a monolithic structure nor a legal entity - can be particularly confusing.

The fragmentation of decision-making in this area (which some would argue is a necessary consequence of a devolved system of healthcare i.e. where health boards or authorities decide on the priorities etc for their region, and primary care practitioners are contractors essentially running their own business) is exacerbated by the persuasive nature of the health professionals' regulatory and professional bodies, which can result in an Information Commissioner's Office (ICO), Government, British Medical Association (BMA) and General Medical Council (GMC) opinion on a particular subject e.g. confidentiality. Across Scotland, however, NHS Boards are required to provide, and show continuing improvement in the provision of staff information governance awareness-raising and training.[12] Also the Chief Scientist Office (CSO)/Government

---

Technology Committee 2nd Report of Session 2008–09 'Genomic Medicine' accessible at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[11] European Commission Review of the Data Protection Legal Framework see http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

[12] NHS National Services Scotland (2005) 'NHS Information Governance Standards' accessible at - http://www.shb.scot.nhs.uk/initiatives/informationgovernance/documents/IG_Standards_FINAL_22122005.pdf (see in particular reference 3e1, 1.004.

research governance framework and its infrastructure do not necessarily dovetail with those of information governance.[13]

1.5 How the rest of the paper is organised

The remainder of the report begins with a closer look at the ethical considerations at stake in the current governance framework. Next, an explanation of the different governance models to be considered is offered, followed by an overview of the current legal landscape. A key feature of the report is the formulation of a template - the GIA (governance impact assessment) - against which to assess current practice and future governance models. Finally, problems and potential solutions for the future are identified. The report concludes by offering recommendations for modifications to the current governance framework.

Chapter 2 The ethical and social considerations and principles relevant to the Information Governance debate

Key Questions addressed by this chapter:

- What are the ethical and social considerations at stake in the context of PII use in medical research?
- What are the relationships between the key principles?
- Which key principles must be given consideration in order to reach optimal governance in this context and how can this be achieved?

Key Messages from this chapter:

- Respect for patient privacy is a core guiding principle and must be central in any governance regime but this is not an absolute ethical or legal value.
- Patient consent serves as a device to show respect to individuals and their wishes; complications arise where consent cannot be obtained but it should not be thought that consent is always necessary either in ethical or legal terms.

[13] Scottish Executive Health Department (2006) 'Research Governance Framework for Health and Community Care', see http://www.cso.scot.nhs.uk/publications/ResGov/Framework/RGFEdTwo.pdf

- Individual privacy rights and obligations to obtain consent should be balanced with the competing concern of the public interest e.g. the potential health benefit of the research to the wider population
- Proportionate governance is essential for the successful functioning of the current landscape governing data uses for research.
- Public engagement is essential for raising public confidence in the use of PII for medical research; this includes raising awareness of the uses of PII for research and the potential associated benefits as well as ensuring high standards of privacy are met by those handling PII by trying to meet expectations around privacy.

The ethical and social considerations apparent in the context of using PII for medical research are varying in nature. It is important to understand the different principles at stake, especially in order to be able to identify problems with the current regulatory framework. Further, familiarity with the key concepts below will demonstrate how complex the interrelationships between competing interests are, and it is hoped, assist in reaching a solution of 'optimal governance' which encompasses as many as possible (if not all) of these key considerations in an appropriate matrix.

Privacy

The notion of privacy - or rather the individual's right to respect for privacy - is not a concept specific only to this particular context.[14] Privacy is important because individuals are important and one's privacy is an integral part of one's life and identity. To fail to respect privacy is to fail to respect the individual. The individual's right to respect for his/her private life and family life is guaranteed under Article 8 of the European Convention on Human Rights (ECHR) and in the UK, by the Human Rights Act 1998. This concept relates to the idea that there is a realm of private information (and conduct), often sensitive in nature, and that it is for the individual to determine whether or not to disclose this data, to whom, and on what basis.

[14] For a full discussion see G Laurie, *Genetic Privacy: A Challenge to Medico-legal Norms* (2002, Cambridge University Press).

This having been said, the right to respect for private and family life as it is referred to in the ECHR, is one of the instances where this right may be encroached upon is where it is in the public interest to do so, a concept to which we now turn.

The Public Interest

The rights and freedoms of others are also important and protected as a matter of human rights. As individuals, we share an interest in the proper protection and advancement of the public interest, thus at times individual interests such as privacy and the wider public interest in the use of data for research must yield to one another. Of relevance here, is the use of the public interest justification most specifically in terms of interest in public health.

Thus those using PII without an individual's consent may argue that the potential benefits to the health of the population at large justify potential encroachments on privacy. Additionally, public health has been used to justify interference with the right of privacy, the most recent example being the Public Health Scotland Act 2008. 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'.[15]

Striking a balance

The problem here, a recurring one, is that of maintaining adequate respect for the individual's right to respect for privacy while allowing the pursuit of the public interest. PAC points out that when considering the use of PII for medical research, 'public interest' should be interpreted 'both to encourage good medical research[16] and 'to protect patient privacy'.[17] As we discuss below, if individuals do not have confidence in a governance system they will be disinclined to participate and this could undermine the whole system - ultimately serving no interests whatsoever. Thus it is meaningful to

[15] 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

[16] 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

[17] Ibid

claim that adequate protection of privacy interests is, in itself, a form of the public interest. The balance to be struck is there between the public interest in adequately respecting privacy and the public interest in promoting sound medical research.

Proportionality

The rights culture in which we live requires that any interference with individual rights be justified and legitimate. While interference might on occasion be appropriate, 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.

Thus we see that proportionality has a central role to play. Indeed, 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 that use of personal data in 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. In other words, the level of scrutiny against which an action is being judged should be appropriate to the risks that such action may give rise to. For example, if a researcher is wishing to link datasets where patient identification is a highly unlikely outcome, then they should not be subjected to the same level of scrutiny as a researcher wishing to link datasets with a higher possibility of identification. Similarly, proportionate governance strives to protect privacy, thus where there is clearly a high risk of re-identification/disclosive output resulting from a linkage, there should be a higher governance burden to meet. Proportionality – linked to risk – is a key feature of good governance.

Scotland lacks definitive guidance on whether use of PII in medical research would be covered by 'public interest'. For example, there are no legal rulings on the matter. This adds to existing confusion on how best to weigh up these competing considerations. While many individuals would have no problems with their PII being used for medical research, others do not wish this information to be shared. This brings us to the role of consent and the ethical principle of respect for autonomy.

Consent/ Autonomy

The notion of consent is central to this topic. As we have argued elsewhere: '[i]t is undeniable that consent remains the primary policy device in legitimating medical research'.[18] In broad terms, the imperative to obtain consent is based on the premise that individuals should have the right to determine what happens to them and by corollary in this particular context, the notion can be narrowed
down to the right to determine what one's PII is used for. 'Consent' in this context raises many different issues.

It is worthwhile noting that another reason why consent is a key consideration is because of the common law duty of confidentiality. Whilst the DPA does not require that consent is obtained to make the processing of personal data lawful, the common law does seem to require some form of consent to information disclosure. It does not, however, demand explicit and fully-informed consent - implied consent may be adequate, as clarified by ICO guidance on the use and disclosure of health data.[19]

Informed consent implies that patients should be 'fully' or 'adequately' informed as to what they are voluntarily consenting to, i.e. to what use the data will be put. The Confidentiality and Security Advisory Group for Scotland (CSAGS) defined this as '[d]irections expressed by the patient indicating the terms on which their personal information may be disclosed, and what and where data may not be disclosed.'[20] However, this is not a straightforward task. First is the problem of determining how much information to give the patient before they can be said to be adequately informed; it is a fact that not all patients will understand or want to hear about the intricacies of a particular research process.

The Article 29 Working Party recently released its Opinion on the definition of consent, where it is recommended that consent must be specific in order to be valid. In the

[18] Mason JK, Laurie GT (2010) 'Law and Medical Ethics, 8th Edition', Oxford University Press at 639

[19] Information Commissioner's Office (2002) Chapter 4, 'Use and Disclosure of Health Data, Guidance on the application of the Data Protection Act 1998' accessible at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf

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

context of secondary uses of data for research, in situations where the exact purpose is not specified, then blanket consent is considered to be invalid. Consent must, according to the Working Party, refer clearly and precisely to the scope and the consequences of the data processing. Thus, consent cannot be informed unless it is specific.
However, the Working Party also appreciates that consent does not always provide a strong basis for justifying the processing of personal data, this being particularly true in those situations where consent is stretched to fit uses for which the consent was not initially provided.[21]

This Opinion also begs questions about the role of broad consent. Thus, whereas blanket consent is an attempt to forego adequately information and is thought to be inappropriate in data protection terms, broad consent is a different beast. A person might agree broadly to a proposition about using or sharing her data when part of the proposition is that she cannot be informed *at the present time* about future uses; however, broad consent is dependent on the data subject being informed *in due course* of things done with her data and/or with the project using her data. Blanket consent involves no such on-going opportunity to be informed. Broad consent is used heavily in biobanking projects where up-front informedness is simply impossible This does not, however, absolve biobankers of a continuing obligation to keep participants informed so that they might, for example, withdraw from the project if it is used in ways that displease them.[22]

How much information is enough?
CSAGS states advised: *'To be valid, a patient's consent must be informed and freely given. In some cases however, it should be reasonable to assume that actions imply informed consent and explicit consent will not be required. Even where explicit consent is required, it may not be necessary for a patient to sign a consent form. What is important is for a patient to have been given a chance to find out how patient identifying information might*

[21] Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
Our thanks to Miss Sarah Sutherland for her help on this point.
[22] On the challenges of biobanking in this and other respects see G Laurie, 'Reflexive Governance in Biobanking: On the Value of Policy Led Approaches and the Need to Recognise the Limits of Law' (2011) 130(3) *Human Genetics* 347-56.

be used and to object if they wish. The use of a consent form is merely one way to provide evidence of this process. '[23]

In relation to the CSAGS approach, the NHS must be able to reassure itself that it has at least implied consent for what it does.

There are clearly situations where informed consent cannot be ***given***, for example, where PII relates to incapacitated adults or children. Further, it is important to note that consent cannot always be ***obtained***, in certain circumstances it is not possible e.g. where patients are deceased[24] or cannot be traced because they have moved away. In other instances, while consent could be obtained, it may not be practical to do so,[25] for example, where the participant group is so large that researchers could not afford the time or money[26] to call each participant to obtain consent. An additional obstacle to obtaining informed consent is that it is not always possible to envisage all the possible uses to which the PII could be put.[27] This being said, it should be acknowledged that many people would not see such obstacles as good enough reasons not to try to obtain consent.

There are two fundamental questions here:

1) Is consent (always) legally required? The answer is No. It is, for example, only *one* means of legitimating the processing of data under the DPA.[28] People should however be informed of uses of their data and this reflects CSAGS guidance. It is a matter of debate whether patients can be said to implied consent to wider uses of their data if they choose to participate in the National Health Service. Further, the Article 29 Working Party has specifically discussed consent with regards to Electronic Health Records and has stated that concerning consent, 'specific' consent must related to a well defined, concrete situations in which the processing of medical data is envisaged. Thus,

[23] ibid.

[24] Regidor E (2004) 'The use of personal data from medical records and biological materials: ethical perspectives and the basis for legal restrictions in health research' in Social Science and Medicine (54) 1975-1894 at 1976

[25] NHS NSS PAC, 'Guiding Principles and Policy for Decision-Making and Advice see n5

[26] PN Furness and M L Nicholson (2004) 'Obtaining Explicit Consent for the Use of Archival Tissue Samples: Practical Issues' 20 J Med Ethics 561

[27] Regidor (2004) at 1976

[28] As we will discuss later, another legitimate means of processing data is under Schedule 3 of the Data Protection Act which allows for processing of data where it is necessary for medical purposes.

'general agreement' of the data subject to future transfer, would not constitute valid legal consent.[29]

2) Is consent ethically required, or at least desirable? It should be noted that consent is not an ethical end in itself but rather a means to an end and that end is respect for individuals and their interests. There may, therefore, be other ways to achieve this without the need for consent. There might also be good reasons in some cases not to seek consent so long as respect is forthcoming by some other means.

While PAC expresses an expectation that consent will be obtained where PII is used, it recognises that this is not always possible and holds that 'in such circumstances, a clear explanation and justification should be given'. 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.

Anonymisation

Anonymisation is generally understood as the process of removing key identifiers such as names and dates of birth from PII thus rendering the identification of data subjects highly unlikely. In legal terms, identifiability is the key concept in the Data Protection Act 1998 (DPA) in that if personal data are identifiable data then they are caught by the provisions of the law.[30] This concept is discussed in more detail in Chapter 3. It is important to note that the process of anonymisation does not render it impossible to identify the data subject, particularly where sensitive personal information is involved, rather, the process renders identification highly improbable, but the risk of identification still exists. It should also be noted that anonymisation, like consent, is a device for respecting the interests of individuals.

Here, the key message concerning anonymisation is that while preserving patient privacy is a key concern, medical research in the public interest is also a key concern. Anonymisation has the potential to impede legitimate research by rendering the data

[29] Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent para III.A.I Article 2(H) at page 18

[30] The Data Protection Act 1998 is more closely discussed in Chapter 4.

less valuable i.e. robbing it of its 'richness'.[31] In instances where it is argued that anonymisation is inappropriate, PAC requires an explanation and justification for not anonymising data.

Public attitudes and Trust

Public confidence in the use of PII is fundamental. Patients and the general public need the assurance that their PII will be used appropriately, i.e. in a manner which can be justified by arguments such as the public interest and which are acceptable to them or at least to a substantial body of reasonable persons. Where there is no confidence in the use of PII for research, patients will be reluctant to provide consent for use of their data; given that the use of PII without consent is not always justified, a lack of participants in projects could seriously impede the progress of medical research projects.

Recent mishaps in the treatment of PII widely covered by the media have not helped to instil public confidence in the way that PII is handled. [32]

In 'Personal data for public good', the Academy of Medical Sciences highlights the scarcity of 'reliable information on public awareness of, or attitudes to, medical research. Research has largely been concerned with general attitudes to the confidentiality of health data in the context of care and treatment.'[33] CSAGS recommended a public education campaign in Scotland although this never took place as research indicated that the public did not support the use of NHS resources for 'expensive publicity'.[34]

[31] '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' CSAGS (2001)

[32] See following - Hi-Tech Scotland (2009) 'Scottish public lose faith in UK Government's data-handling' accessed at http://www.hi-techscotland.com/article/09-02-09__scottish-public-lose-faith-in-uk-governments-datahandling; 'The problems continue because of the not infrequent loss of useful data that accompanies anonymisation' Mason and Laurie (2006) see n8 at 683;
Cabinet Office (2008) 'Cabinet Secretary publishes plan to improve data security' accessed at http://www.cabinetoffice.gov.uk/newsroom/news_releases/2008/080625_data_security.aspx ; Harrison (2008) 'Government's record year of data loss' accessed at http://www.telegraph.co.uk/news/newstopics/politics/1574687/Governments-record-year-of-data-loss.html

[33] The Academy of Medical Sciences (2006) 'Personal Data for public good: using health information in medical research' (2006) at 69 accessible at www.acmedsci.ac.uk/download.php?file=/images/project/Personal.pdf

[34] Scottish Executive Health Department, NHS HDL (2003) 37, ' The use of personal health information in NHSScotland to support patient care.' See http://www.sehd.scot.nhs.uk/mels/hdl2003_37.pdf at p6.

This points to the need for further research around specific issues related to research using personal data. The Public Engagement stream of SHIP is carrying out research in order to gain more insight into public attitudes towards the use of PII.

It should however be noted that numerous efforts have been made to improve information on research to patients.[35] Moreover, the Information Governance Standards imposed on NHS Boards via the Clinical Governance and Risk Management (CGRM) standards of NHS Quality Improvement Scotland have 2 standards around the adequate informing of patients. Boards are required to have improvement plans in relation to all of their standards and are 'inspected' every 3 years.[36]

We can learn valuable lessons from a few studies which have been carried out in this area A recent study commissioned by the Medical Research Council (MRC) to investigate public attitudes regarding the use of personal health information for medical research found that '[p]ublic awareness of the use of personal health information for the purposes of medical research is low. They know that medical research is undertaken, but few have a good understanding of what it entails, who does it, and for what purpose'. [37]

The research highlighted the importance of communication in establishing public trust in the use of PII for medical research: '...if the public is informed about what medical research entails, they are generally positive towards it. The key to effective communication with the public on the subject is the need to keep terminology simple and tailor communications for a lay audience.'[38]

---

[35] For example, the NHS HDL (2003) 37 'The use of personal health information in NHS Scotland to support patient care' http://www.show.scot.nhs.uk/sehd/mels/HDL2003_37.pdf
Also, the Scottish Government consumer focus project 'Health Rights Information Scotland' was designed to inform patients and one of their key publications is 'Confidentiality – it's your right' which explains how patient information is used.
HPS (Health Protection Scotland) offer a number of informational leaflets on their website accessible at - http://www.hps.scot.nhs.uk/
ISD also offer such information -http://www.isdscotland.org/isd/846.html

[36] Also, there was a national patient information campaign in relation to the Emergency Care Summary (ECS) with the SG contracting with Royal Mail to provide a leaflet to every Scottish household accessible at http://www.scotland.gov.uk/Publications/2006/08/16152132/0

[37] Ipsos MORI (2007) 'Keeping It Confidential: Public Attitudes Towards The Use Of Personal Health Information In Medical Research', accessed at http://www.marketresearchworld.net/index.php?option=com_content&task=view&id=1498&Itemid=77

[38] Ibid

A study supporting the public tendency towards supporting research once awareness of its purpose has been raised is illustrated by Barrett et al. They found that awareness of cancer registries was low; however, once those questioned were made aware of such registries, they gave wide support for making cancer registries statutory.[39]

One recent consultation report concluded that: '[i]t is clear that the public expects their consent to be sought if the data used is identifiable'. In fact, the same consultation found that a considerable proportion of participants would prefer their consent to be obtained even where anonymous data was to be used.[40]
So public engagement is essential although it can often provide conflicting results.

Engagement exercises might include:
1) raising public awareness of medical research, its uses and potential benefits, and
2) communicating this information in an audience appropriate manner, and
3) "the demonstration of high standards of research practice."[41]

The Public Engagement arm of the SHIP Project is involved with implementing these important steps. To date, it has carried out research on public attitudes to data sharing for research purposes. The focus group findings indicated that control, confidentiality and trust were important considerations. The limitations of consent and anonymisation were acknowledged to some extent, however there was a lack of understanding of the complexities involved with the process of anonymisation. It became clear that more work needs to be carried out, particularly in order to explore what alternative options of control (other than upfront consent or opt-in)are available and whether the public considers that consent is the only means of exercising control. The focus group findings also indicated that trust was very important and in particular, trust in who controlled and accessed personal data.

[39] Barrett G et al (2006) 'National survey of British public's views on use of identifiable medical data by the National Cancer Registry' BMJ 332:1068-1072
[40] Department of Health (2009) Consultation Report : 'Consultation on the additional uses of patient data' accessible at http://www.dh.gov.uk/en/Consultations/Responsestoconsultations/DH_109310
[41] Ibid

Subsequently, a workshop was held in order to gain insight in to researcher attitudes towards trust. In future publications we will discuss the Public Engagement findings and the implications which these have for governance mechanisms within projects like SHIP.

To answer the question of what constitutes a high standard of research practice we must appreciate that it relates to how well the ethical principles outlined above are respected and balanced in practical terms, and thus potential models which SHIP would adopt could be judged against how well they consider these principles and encompass them.

In summary, key messages from this chapter are -

- There is a public interest both in advancing medical research and in ensuring adequate protection of individual privacy and these should be balanced against each other.
- Whilst consent is a central theme in the debate, problems around obtaining consent exist, particularly; it is not always possible to obtain consent. Further, even where consent can be obtained, the question of how much information is needed before 'fully informed consent' can be given remains.
- Obligations to obtain consent should be balanced with the public interest in research.
- Proportionate governance is important and necessitates a balance between the level of scrutiny against which a procedure is held and the likely risks related to the procedure.
- Anonymisation of PII is an option for data usage without consent where an authorising body such as PAC has approved the use. The process of anonymisation however, has its own limitations, particularly in that information can never fully be anonymised.
- Public engagement is essential for raising public confidence in the use of PII for medical research, this includes education on the uses of PII for medical research and information gathering on what the public expects from the use of their PII in this area.

Chapter 3 Achieving the objectives of this research stream

Key Questions addressed by this chapter:

- What are the key necessary components for an optimal governance model?
- How can these necessary components be included in such a model?
- What are the governance options available?

Key Messages from this chapter:

- An optimal governance model should embody a coherent, transparent and principled framework; this should follow a proportionate governance approach; it should embody clear and simple protective procedures for researchers to follow.
- An optimal governance model should strive to ensure that high standards of research practice should be met during all aspects of the research process, from procuring PII, to using it, to storing it.
- The performance of Privacy Impact Assessments (PIAs) can be a useful tool in monitoring potential privacy risks prior to the implementation of any particular data sharing model.
- An optimal model would include penalties which whilst not excessive, have enough power to deter researchers from breaching their obligations when handling PII.
- Choice, anonymisation and authorisation-based approaches are available models, however whilst reconciling competing interests in each model can be difficult, these principles are not mutually exclusive. The challenge lies in incorporating appropriate measures at appropriate points in the governance matrix, justifying each by reference to the ethical principles and legal standards at stake.

Prior to establishing the key components which an optimal governance model must possess, we should familiarise ourselves with the approaches available i.e. choice, anonymisation and authorisation based models.

3.1 An explanation of available approaches e.g. anonymisation, authorisation, choice

In terms of how we approach optimal governance, three main theoretical approaches exist, namely those based on anonymisation, authorisation and/or choice. However, before we consider these, it is important to note that varying references to such terminology exist and this can pose problems. For example, 'anonymisation' may refer to either anonymisation or pseudonymisation; 'choice', where it is a synonym for 'consent', may refer to informed consent or implied or explicit consent. Thus, there is a need for clarity of terminology and consistency of use of such terms. It is not for us to dictate which specific terms should be used in each instance or rather, which definition of terms is used, but it is important to establish and consistently maintain terminology which has been commonly acknowledged.

Further, it should be noted that anonymisation, authorisation and consent-based approaches can be considered alone or in combination in offering the best perspective for optimal governance. It is arguable that the best balance is to be found in a combination of all 3 approaches, thus the question is not about excluding any one consideration, but of finding the right fit. We are not discussing here specific models such as safe havens[42] (secure physical locations or a set of administrative agreements for ensuring the safe communication of PII) or MILA (Multi Institutional Linkage and Anonymisation system) based models. Rather, we are concerned with operational approaches to be taken, which, in turn, reflect elements of the technical models being considered for Scotland.

CHOICE

A choice-based approach is one which places the patient or surrogate decision-maker as a central feature of the model. It involves the provision of adequate levels of information to facilitate meaningful choices. An obvious example of this approach is the informed consent approach. An alternative is the opt-out approach which can equally be seen as an "informed refusal" approach.

[42] For more information on Safe Havens see - NHS Connecting for Health accessible at www.connectingforhealth.nhs.uk/systemsandservices/.../safehaven

ANONYMISATION

Anonymisation is often championed as the alternative to a consent/choice-based approach in that it is argued that if data are sufficiently anonymised then consent is not required. There is some legal basis for this view in that the data protection legislation does not apply to anonymised data. A further argument in favour of anonymisation is that this process can largely remove the source of most people's concerns with processing their data, i.e. being identified; thus if this risk is minimised or eliminated then there is no need to seek consent.

AUTHORISATION

Authorisation involves decision-making or advice from a trusted third party - usually a body of persons but it can also involve an individual such as a Caldicott Guardian - to permit the use of patient-identifiable information and/or linkage of data for research and other purposes without consent. Authorisation or advice can be invaluable where consent and anonymisation are impossible or significantly impracticable. The process not only offers scrutiny of the acceptability of what is proposed in terms of linkage (and associated risks), but it can also be a means to assess whether claims are sound that consent or anonymisation cannot be used.

3.2 What are the consequences of choosing one approach over others?

Choice

It should be noted here that the benefits or disadvantages of a choice-based approach depend to a large extent upon which approach is employed by NHS National Services Scotland (NSS) because of its central role in this context[43]. However, we should not ignore the viewpoints of other data controllers or stakeholders such as, Caldicott Guardians and Directors of Public Health, the CHI Advisory Group and the Health Boards, the latter of which will ultimately be swayed by national SG (Scottish Government) policy.

Pros

- Obtaining consent is widely-perceived to legitimate the use of PII in medical research.

[43] As part of NHSNSS, ISD (the Information Statistics Division) acts as leading data custodian on health statistics and statistical disclosure in Scotland.

- Choice can represent evidence of a measure of respect for patient autonomy
- A consent model provides direct control to individuals to refuse uses of their data.

Cons

- Although respect for patient autonomy and the right to privacy must be respected, a choice-based approach whereby informed consent from patients must be obtained prior to using PII may impede research.
- Furthermore, as discussed in Chapter 2, obtaining informed consent is not always possible or practicable. If PII for which informed consent was not obtained cannot be used in any instance, it is possible that pre-existing data would need to be removed from studies.
- Informed consent or even informed refusal models (whereby patients are given the chance to opt out their PII from medical research) work on the assumption that patients are fully informed as to the use of their data and potential benefits. Full informed consent is not achievable in many contexts - for example - when holding data for longitudinal research purposes where we simply do not know what uses it will be put to or by whom.
- Consent-based approaches can bias research results and undermine their overall credibility. Research of self-selecting groups is not necessarily objectively accurate or easily verifiable.
- Consent alone is not adequate to protect the range of an individual's interests in what is done with their PII.

Anonymisation

From the outset, it should be noted that the specific benefits and disadvantages of SHIP using anonymisation for data set linkage will depend on the specific methods of anonymisation which will be employed.

Pros

- Lowrance states: '[a] way out of many problems should be de-identification, or

anonymisation of data. If data are not identifiable the data are not 'personal' and, unless safeguards are compromised, the data-subjects stand only a very low risk of being harmed, which should be the principal point and should obviate the need for express consent. Much, perhaps most, health services research only uses anonymised data.' [44]

- Reversible anonymisation 'which maintains a connection between substantive data and personal identifiers but does not allow researchers to know the identifiers, serves both privacy and researchers well'.
- In fact, reversible anonymisation may be desirable in order to 'allow technical validation or auditing of the data and to avoid duplicate cases; allow requesting additional data if necessary; check consent or ethics committee stipulations; be able to inform the physician or patient of useful findings; and facilitate later research follow-up.'[45]

Cons

- While this may be a popular choice in medical research, many challenges around anonymisation exist.[46] For example, It has been argued that no data can be 'fully anonymised' - 'Names, age, gender, ethnicity, and location (or address), are often removed from research data, but this should not be an arbitrary decision. There is the potential to identify particular participants based on a combination of these features without having access to that individual's name', this is especially the case the more unique such identifying features might be.[47]
- Opinions may differ on what counts as adequate anonymisation (both technically and legally).[48] For example, where data sets are linked, more information on an individual is available and identifiability becomes increasingly possible. The threshold for acceptable anonymisation is not a clear bright line.

[44] Lowrance W (2003) 'Learning from experience : privacy and the secondary use of data in health research' in J Health Serv Res Policy Vol 8 Suppl 1 July 2003 S1:5
[45] ibid
[46] Clark A, ESRC NCRM (Economic and Social Research Council National Centre for Research Methods) Working Paper (2006) 'Anonymising Research Data' considers the issues related to data anonymisation in the social science research however some of the lessons learnt can be extended to our setting of medical research.
[47] Homer et al (2008) 'Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping micro arrays' in Public Library of Science Genetics J 4:e1000167.
[48] n 34 above.

- We should consider whether anonymisation is a viable approach for all kinds of research. Informed consent allows PII to be used, thus leading to often richer data sets yielding more fruitful research results, however where data are anonymised and value can be lost,[49] the potential benefit to the public may be diminished. But in both cases and consent[50] or anonymisation can undermine the validity of research results.

Authorisation

PAC is an example of an authorising body in Scotland, however it should be noted that it is not '***the***' authorising body in Scotland. PAC is an advisory committee to the board of NHS National Services Scotland (NSS) and advises its Caldicott Guardian and Caldicott Guardian to NRS (National Records of Scotland)[51] on uses/linkages/disclosures of personal health data for research uses. NHS Boards release patient data for research uses and use their own authorisation mechanisms for doing so (e.g. application form considered by the Caldicott Guardian for each Health Board). PAC does not authorise on behalf of these other NHS boards, its authority is limited to the datasets of which it is custodian, being the datasets held by NHS ISD and NRS. PAC is a well-established group with a strong track record and it has been suggested that NSS hopes that it is well regarded and a useful model for others. There is currently no legislative basis for this role in Scotland. An equivalent role in England & Wales is performed by the Ethics and Confidentiality Committee under the auspices of the National Information Governance Board and which has a statutory basis for its work (ss 251-252 of the NHS Act 2006).

The Community Health Index Advisory Group (CHIAG)[52] also holds a key advisory role in relation to patient demographics and research uses. CMO (Chief Medical Officer) and Directors of Public Health are its key stakeholders but the substantive data controllers (the NHS boards) retain ultimate authority for their decisions.

[49] The Academy of Medical Sciences, 'Personal data for public good: using health information in medical research' (2006)
[50] Al-Shahi R, Vousden C and Warlow C 'Bias from requiring explicit consent from all participants in observational research: prospective, population based study' *BMJ 2005;331:942*
[51] NRS was formerly GROS (General Register Office for Scotland)
[52] Community Health Index Advisory Group. See http://www.shsc.scot.nhs.uk/shsc/default.asp?p=108

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.

Pros

- While PAC is said only to advise, it could be argued that essentially it serves the same purpose of legitimating PII use without consent, given that ISD and NRS rely heavily on PAC.[53]
- Authorising or advisory bodies can bring an element of expertise and independent scrutiny to difficult decisions involving the release and use of PII.
- Appropriately-constituted and trusted bodies can serve an important role in maintaining and fostering trust in governance mechanisms
- Such bodies can call into question the claim that consent/anonymisation are not possible or desirable and can encourage these routes if thought to be more acceptable.

Cons

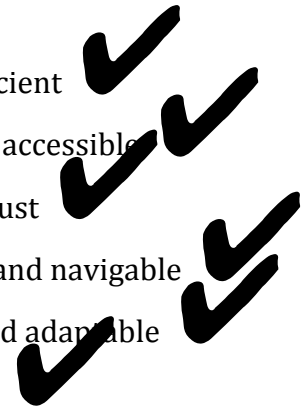
- Authorisation can be problematic in that those in the position of authority assume to know what the public would or would not tolerate as acceptable use of their PII in medical research. Thus this process can be said to negate the importance of choice. This argument can be supported further by a purported lack of information held on public attitudes to the use of PII for medical research.[54]
- PAC lacks statutory authority and thus legislative change may be necessary. More particularly, the remit of PAC is restricted to ISD and NRS.

[53] However it should be noted that NSS and NRS also look for evidence of authority from other Boards where data streams originating other than ISD/NRS are involved in a research proposal.
[54] The Academy of Medical Sciences at 69, see n25

- The centralisation of power in one or a few authorising bodies might not work in the public interest nor does it necessarily guarantee adequate protection of individual interests.
-

3.3 What does optimal governance look like?

We suggest that the most useful approach in understanding what optimal governance might look like is by establishing necessary key questions to ask of a governance model and by determining how well different models do or do not answer these questions. In this way, we can develop a template to help us assess the robustness and appropriateness of any given approach to, or model of, information governance. Furthermore, any robust governance model should be sufficiently sensitive to, and protective of the ethical and social values and principles at stake. It should, ideally, makes explicit said values and principles as the basis upon which the entire governance edifice rests. This is not to suggest that there is one correct approach or correct set of principles; rather it is to posit that a governance matrix must demonstrate these features as a minimum. Their particular configuration then becomes a matter of dialogue, debate and justification. It goes without saying that all legal requirements must be met. As a minimum, an optimal governance framework would be able to meet the following checklist:



- Effective and efficient
- Transparent and accessible
- Procedurally robust
- Understandable and navigable
- Proportionate and adaptable
- Legal and ethical
- Principled ? Adaptive? Reflexive?

This last point leaves questions open about how best to construct the basis of any given model. As stated above, 'optimal' does not imply 'uniform'. We explore in future

working papers how these elements might best be deployed in the context of SHIP. For now, the following key questions allow us to construct a template of assessment of existing governance mechanisms and a basis to construct new ones.

Key questions to be answered

These questions have been developed as a result of our research involving the primary and secondary literature and from dialogue with key stakeholders involved in research information governance and with researchers themselves.

1) Is the model fit for the purposes that it is designed to achieve, now and in the future?

As discussed previously, any model must serve a range of purposes; first and foremost, robust privacy protection must be provided while facilitating scientifically sound and ethically justified research. How are these elements assessed and managed within the model? What role, if any, is played by consent, anonymisation and authorisation? What are their relative interactions and how is this balance justified? If any element is missing, why and how is this justified?

2) How does the model reflect public expectations and impact on public confidence?

As outlined in Chapter 2, particularly with regards to privacy and consent and the important balance which needs to be met between the two, any framework must pay due consideration to these issues and promote respect for them. High standards of research practice should be met during all aspects of the research process, from procuring PII, to using it, to storing it. This is not only essential in avoiding penalties for inappropriate processing of PII, but also, to raise public confidence in the use of such data for medical research.

3) How does the model fare when subject to a PIA (Privacy Impact Assessment)?

The performance of Privacy Impact Assessments (PIAs) can be a useful tool in monitoring potential privacy risks prior to the implementation of a data sharing model. These exercises allow those involved to assess the potential risks of any procedure/linkages. The carrying out of PIAs should become the norm amongst the basic procedures carried out during research; in fact, it is envisaged that these will

become basically mandatory. The most likely public sector mechanism for making PIAs mandatory will flow from the Scottish Government Privacy Principles consultation[55]. It should be noted, that a PIA is a tool to be tailored according to the particular model under assessment. The ICO has created a PIA Handbook to 'help organisations assess and identify any privacy concerns (a Privacy Impact Assessment) and address them at an early stage, rather than leaving the solutions to bolt on as an expensive afterthought.'[56] An important related privacy issue is whether or not datasets are disclosive, although this seems like an obvious question, we need to ensure that any model employed will ensure that re-identification is only possible under specific pre-determined circumstances i.e. clinical trials, and that in all other instances, risk of re-identification is minimal.

4) How is the model monitored/regulated?

For example, how are key actors involved regulated? Should individual data controllers police their own datasets or is there a role for a body with over-arching remit and authority? For example, in the Scottish context is there any need for a 'Super-PAC' or a similar body charged with oversight of all linkage applications? Is this feasible? How do we decide how much of the dataset will be released via the agent and what data view will be provided? How are conflicts of interest avoided and in particular is it desirable to avoid having actors with more than one role? For example while Scotland is relatively small, will it be possible to segregate duties? How will the segregation of roles be controlled? E.g. is it acceptable that one person or entity could have both custodial and analytical roles?

5) Do all parties involved understand the implications of the particular model?

Whose safe haven or dataset is it? Upon whom does primary (legal) responsibility lie? What happens to liability when data are shared? This needs to be clear from the outset. Furthermore, an optimal model would have clear and simple procedures for researchers seeking data. Guidelines would be clear for all involved in dealing with PII.

[55] Scottish Government (2009), 'Privacy and Public Confidence in Scottish Public Services: draft Identity Management and Privacy Principles'. See http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation

[56] Information Commissioner's Office (2009) , 'Privacy Impact Assessment', Handbook - accessible at http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

It is desirable that the interrelationships between the various legal actors, instruments and guidance are complimentary to one another as opposed to conflicting/confusing.

6) What vetting and training methods will be implemented in any model?

The training methods most appropriate for any one model should be considered. Also, we need to ask what is required from potential data recipients when their requests are being considered. What are the pros and cons of a model of approved researchers?

7) Is there accountability in the model and who is accountable at each stage in any model?

This includes consideration of the status of data on the journey from source to ultimate use e.g. whether they are anonymised/pseudonymised and who carries this out, for which purposes and for transfer to whom. This also involves considering the responsibilities for data holding/usage e.g. who is hosting the agent and the safe havens? Will data be held or used within/out with the NHS? Researchers in academic institutions might spend months working on particular studies in the facility of a project whereby the facility becomes their permanent workplace. When considering data usage, the incorporation of highly decentralised governance models where secure labs might be provided on university campuses should be considered.

The issue of accountability relates not only to who is accountable at different stages but also what they are accountable for, and this should be clearly established and understood by all involved.[57] The ICO (Information Commissioner's Office) is often criticised for its lack of enforcement powers, relying heavily on voluntary compliance with the laws governing the use of PII, calls for a larger deterrence factor or, 'more teeth' were widely made.[58]Following substantial lobbying, the ICO has been granted with the power to enforce monetary penalties for up to £500,000 however whether or not these powers are actually used, and to what extent remains to be seen. An optimal model would include penalties which whilst not excessive, have enough power to deter

[57] For example, QResearch (an extensive database of anonymised health records) sets out a condition in its access protocol that one of the core research teams in any project accessing the data needs to be GMC registered so that they can be held accountable for breaching professional standards if a member of the whole team breaches confidentiality or any other condition given in the protocol.

[58] See Chapter 4 for more detailed discussion on this.

researchers from breaching their obligations when handling PII. In fact, in recent months, the ICO has made use of these new powers, fining £100,000 and £60,000 respectively for each data protection breach. The first case involved sensitive information being incorrectly faxed to the wrong number (twice). The latter involved an employee taking home an unencrypted laptop which carried personal details of some 24,000 individuals, and which was subsequently stolen by thieves.[59] It should be noted that no distinction has been made between the public and private sector when issuing these penalties, thus health boards are just as much at risk for receiving penalties than private bodies.

8) Who are the stakeholders and are they satisfied?

Key stakeholders which have been identified include researchers, ISD, Health Boards, Caldicott Guardians, health professionals, GPs (acting in a self-employed capacity where attempts are made to foster a relationship between ISD and the GP research network in Scotland) and international applicants for data. Publics must also be added to this list. Clearly, for any model to be a success it must satisfy interests of all stakeholders. However, it should be noted that it is not possible to identify all stakeholders in the project, particularly because we cannot envisage all of the potential linkages which may take place. This requires an on-going process on monitoring stakeholders, their interests and their expectations, all of which can change over time. A robust governance mechanism is one which is capable of adapting to and accommodating such shifts.

9) How does the model sit within the legal order?

It is trite to confirm that any governance system must comply with the law, but the law itself is not always clear in its application. Thus questions must be asked, such as: is further legal reform/clarification required? Further key questions which arise in this area include: who is the 'data controller' in terms of the law and what are their responsibilities, liabilities and rights? What kinds of terms are permissible in data sharing arrangements and how far can issues of liability be negotiated and agreed between data sharing parties? What about data transfers with 3rd countries? Transfer outside of EEA countries must be considered.

[59] Joseph Miller & Co Chartered Accountants, 'First Data Protection Act fines issued'(2011) see http://www.joseph-miller.co.uk/ard/enews_article.asp?ID=2278&AID=816&CID=1

One area of potential legal reform for Scotland is the question of whether it requires a statutory authorising body. The Privacy Advisory Committee in Scotland lacks statutory authority despite the influential role it plays and the rather important responsibilities that it fulfils. The question of introducing a new body or instilling the pre-existing PAC with statutory authority is raised.

10) Does the model add value to and improve upon the inadequacies of existing mechanisms?

While it is acknowledged that no governance model will be perfect and compromises must be made, one necessary component is that the new model improves upon key inefficiencies present with the current one. Not all parties are likely to be satisfied with change and not all stakeholder interests will be met by any one governance model. This therefore requires detailed discussion, negotiation and agreement on the values and objectives which the model is designed to promote and also articulation and acceptance of any compromises that are to be made. Chapter 5 tests the current model against these considerations.

11) Does the model reflect a proportionate approach to governance?

As noted previously, proportionality is integral to optimal governance. The governance mechanisms which must be fulfilled in any case should be proportionate to the potential risks associated with a procedure. An overly burdensome governance regime will stand in the way of achieving the benefits of data linkage. Whilst we recognise that governance is fundamental for protecting the diverse values at stake, these values can be protected whilst at the same time avoiding unnecessary hurdles.

Template upon which to test current and potential models

Having discussed the necessary questions, we can use these as a template against which to text the pre-existing and potential models with regards to how well they respond to the requirements of our envisaged governance model. Thus, key questions to ask are:

1) Is the model fit for the purposes that it is designed to achieve, now and in the future?

2) How does the model reflect public expectations and impact on public confidence?

3) How does the model fare when subject to a PIA (Privacy Impact Assessment)?

4) How is the model monitored/regulated?

5) Do all parties involved understand the implications of the particular model?

6) What vetting and training methods will be implemented in any model?

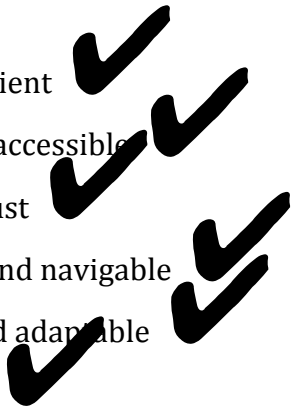
7) Is there accountability in the model and who is accountable at each stage in any model?

8) Who are the stakeholders and are they satisfied?

9) How does the model sit within the legal order?

10) Does the model add value to and improve upon the inadequacies of existing mechanisms?

11) Does the model reflect a proportionate approach to governance?
Overarchingly, we are looking for a system which is:



- Effective and efficient
- Transparent and accessible
- Procedurally robust
- Understandable and navigable
- Proportionate and adaptable
- Legal and ethical

Part 2 – Where we are now? The current landscape

Chapter 4: An outline of the current legislative framework

Key Questions addressed by this chapter:

- As the potential for medical research advances, those dealing with PII are continually seeking clarification on the law and processes for data handling. What is the current legal framework governing this area?
- What are the key legal instruments and guidelines concerned with PII usage for medical research?
- Who are the key actors and decision makers?
- How can the 'power, status, roles and interrelationships of the regulatory actors with "formal" authority'[60] to regulate medical research be described and understood?
- What future changes may occur in the regulatory landscape, and what effects might they have on the dynamics of the current framework?

Key Messages from this chapter:

- The governance of the use of person identifiable information (PII) in medical research differs in England and Scotland, however, despite the differences which will be outlined below governance in both areas is sub-optimal and can be improved upon. Lessons for Scotland may be learned from the English experience and vice versa.
- The lawfulness of the use of PII in Scotland depends on compliance with the Data Protection Act 1998, the Human Rights Act 1998 and the common law of confidentiality.
- In addition to legislative requirements, professional guidance and NHS policy such as the Caldicott Principles may also affect the use of PII.
- The current governance framework is unsatisfactory, with unclear legislation and professional guidelines which are often conflicting in nature. Perhaps the

[60] Kaye and Gibbons (2008) at 117

time has come to modify the current governance landscape and introduce a more coherent and proportionate framework.

Whilst this chapter offers an outline of the current governance framework, where applicable, it also identifies the various individuals who are subject to specific laws as well as the consequences of non-adherence to these laws.

4.1 Key legislation (the documentary governance framework)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The Directive governs the processing of personal data within the European Union (and the wider European Economic Area (EEA)). It defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, social or cultural identity'.[61] It provides that in determining whether a person is identifiable, *'account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'*.[62] (Here, such data is referred to as PII - person identifiable information).

Directives represent important legal instruments for the European Union[63]. Relevant Member States enjoy leeway regarding how they achieve the intended objectives of the directive; however achieving the intended results of the directive is a legally binding obligation on Member States. In acknowledging the increased flow of and technological progress in the handling of personal data between Member States, the Data Protection Directive sets out 3 main objectives, these being :

1. Harmonisation of differing Member State laws;

[61] Data Protection Directive 95/46/EC

[62] Ibid

[63] The DPD recommendation is particularly relevant to the handling of medical data, of note, it stipulates that 'medical data should be collected and processed only by health-care professionals' however it should be noted that this is merely a recommendation and not law.

2. Harmonised laws should facilitate further cooperation and coordination of data sharing;
3. The need to protect the rights of the data subjects, particularly the right to respect for private life as guaranteed under Art 8 ECHR.

The Directive does not however, apply to data 'rendered anonymous in such a way that the data subject is no longer identifiable.'[64] Procedures for rendering data anonymous are discussed in Chapter 5. However as we have mentioned, it is highly unlikely that linked data is fully anonymous so as to render identification impossible, but rather that it has been anonymised to a *relative* degree, i.e., it is not likely reasonably that someone will be identified from the data.

The Directive does provide Member States with 'a margin of manoeuvre' allowing them to 'specify in their national law the general conditions governing the lawfulness of data processing' whilst, at the same time encouraging them to 'seek to ensure a high level of protection in the Community'.[65]
The Directive has been implemented in the UK by the DPA 1998, discussed below however note that the Directive is currently under review, and it remains to be seen whether amendments will be more accommodating of data sharing and whether the Directive will offer more definitive guidance to data and it's handling in the eHealth context.

Key points to note here are:

- Privacy protection is important but the sharing of data is also a key objective of the Directive
- Processing and sharing of data must comply with 8 key data protection principles laid down in the Directive and which must be embodied in domestic laws.
- Member States have a degree of flexibility in how they regulate the processing of data. In particular, consent to processing it not an absolute legal requirement

[64] Ibid.
[65] Ibid

and processing can be justified in the 'substantial public interest' without the need for explicit consent.

Human Rights Act 1998 (HRA)

The UK enacted the Human Rights Act (HRA) in 1998. Article 8(1) provides that the UK must recognise and respect the individual's right to respect for private life whilst Article 8(2) provides that as this right is not absolute in nature, it should be balanced with other interests, such as the protection of health or the protection of the rights and freedoms of others.[66]

It follows that if it is possible to establish that the particular use of PII in question does fall within Article 8(2) i.e. in the interest of the protection of health or the protection of the rights and freedoms of others, the courts can determine that there has not been a breach of the human right to respect for private life. In making this determination the court will ask whether the impact of the use of the information upon an individual's private life was *proportionate* and *necessary* in pursuance of the protection of the interests under Article 8(2). However, it should be noted that whether or not use of PII without consent falls under Article 8(2) is a disputed matter.

What, then, counts as necessary and proportionate use of PII? Standard ECHR (European Court of Human Rights) jurisprudence[67] demands certain key elements for a measure to be deemed necessary and proportionate where Article 8 interference is alleged. The measure must demonstrate that -

a) it addresses a 'pressing social need'

b) its operation is proportionate and

c) the reasons advanced for its existence are 'relevant and sufficient'.

1) Who is responsible?

[66] Human Rights Act 1998 Article 8 Right to respect for private and family life
(8)1 everyone has the right to respect for his private and family life, his home and his correspondence.
(8)2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[67] *Handyside v United Kingdom* (*1976*) 1 EHRR 737

Anyone acting in a way which engages human rights must justify their conduct in doing so. The entire SHIP enterprise and anyone else handling PII must justify their dealing with personal data.

2) What are they responsible for?

For giving due respect to human rights considerations, particularly Article 8 considerations regarding respect for private life, examples of due respect might include obtaining patient consent or anonymising data so as to minimise risks of reidentification.

3) What are the penalties?

Breaching the HRA means that those infringing an individual's rights may be liable to pay damages which the court deems fit to provide the applicant with just satisfaction. Whether or not damages will be awarded, and to what extent, is for the court's determination. The court may also decide against awarding damages, and may prefer for example, in this case, that the data handling procedures of the authority be reviewed. A prohibition on further use of information by the grant of an injunction (England and Wales) or interdict (Scotland) is also possible.

4) What are the flexibilities?

Those whose conduct engages the right to respect for private life must establish that the conduct falls within Article 8(2) and justify their actions by proving that their behaviour was necessary and proportionate, as defined above.

5) What is the role of consent, anonymisation and authorisation?

Arguably, it is a demonstration of respect to individual's private life to seek their consent before processing their data. Furthermore, anonymisation is a proportionate measure to minimise any likely harms; the argument of necessity being that it is necessary to process data without consent in order to carry out socially useful research.
In the context of authorisation, the argument might be put that the encroachment upon the right to respect for private life is proportionate and necessary, the balance of benefits and harms being carried out by a responsible authorising body. While this has

never been tested in court, if successfully argued then an individual would avoid penalties for an Article 8 infringement.

Data Protection Act 1998 (DPA)

The DPA is based on 8 principles of data protection. It identifies the key entity responsible under this law to be the data controller (DC). Under the DPA 1998, a data controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.' Data processors refer to all individuals involved with handling data. It should be noted that Data Processors when referred to in the DPA context, act only on the instructions of Data Controllers who retain accountability for safe use of personal data through its processing life. Data controller and data processor roles are crucial in the determination of legal liability in this entire area however despite the definitions provided by the DPA, identifying these key actors has proven difficult in practice, beyond the UK and amongst other Member States under the European Directive.

In recognition of these inherent difficulties for Member States in respectively identifying data controllers and data processors, The Article 29 Data Protection Working Party drafted guidance specifically on this issue. It defines the concept of a data controller as 'autonomous, in the sense that it should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis'. The existence of a data processor is deemed to be dependent on decisions taken by the data controller as to how data should be processed and by whom. Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.[68]

The Data Protection Act demands 'fair processing' of data, which requires bodies processing personal data to explain what information they hold and what it is used for. Originally, this information was covered in an FPN (Fair Processing Notice) however,

[68] Ibid

the Information Commissioner has recommended that the term is replaced by PN (Privacy Notice) and offers a code of practice for guidance on how to carry these out.[69] According to the code, 'the duty to actively communicate a privacy notice is strongest where the intended use of the information will be unexpected or objectionable, or where the information is confidential or particularly sensitive.' Thus, informing the public in the context of PII in the health setting is very important. This being said, determining how much information is enough and who decides that the information provided should be adequate are difficult questions.[70]

Examples of desirable/effective Privacy Notices in the health context might include -

- A large poster in a hospital or surgery next to the reception area outlining that data MAY be used for research and if so, the patient would be contacted regarding this.

- A leaflet given to every new patient registering with a surgery. The leaflet would contain all of the purposes for which the data will be used and a statement indicating that the patient will be contacted if the data is needed for additional purposes.

Examples of undesirable/insufficient Privacy Notices might include -

- A notice saying: "we are going to process your data for your own good"

- In a community that consists to 80% of British citizens of Pakistani background, a notice only written in English.

[69] ICO Privacy Notices Code of Practice accessible at http://www.ico.gov.uk/for_organisations/topic_specific_guides/privacy_notices.aspx

[70] In the US, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires informed consent forms for research studies to include detailed information on how an individuals privacy rights will be protected - for more information see http://www.hipaaguide.net/

Section 1 DPA stipulates that each DC, must process 'sensitive personal data' (which includes information as to an individual's 'physical or mental health or condition' in accordance with both Schedules 2 and 3 of the Act.

The first data protection principle states that data should be processed fairly and lawfully. Relating to this principle, Schedule 2 governs the processing of any data and conditions relevant to fair and lawful processing e.g. where processing is with the data subject's consent, where processing is necessary to 'protect the vital interests of the data subject' etc. The NHS relies particularly upon Schedule 2 para 6(1) - where processing is 'necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.'

Schedule 3 is equally relevant to the 1st principle conditions which are in turn particularly relevant to health data –

a) necessary for medical purpose
b) with explicit patient consent

It is important to note the usage of the word 'necessary', suggesting that if alternative methods may be used to achieve the same aim, methods which avoid processing personal data, these should be used instead, the most obvious example here is where personal data can be anonymised.[71] It is important to remember that each time a patient record is processed; the necessity test must be fulfilled.

Further, it should also be noted that 'medical purpose' includes the purposes of 'preventative medicine, medical diagnosis, medical research[72], the provision of care and treatment and the management of healthcare services.' (Schedule 3, s8 (2))

Data Protection - Key messages

[71] For an overview of the process of anonymisation and a discussion of the benefits and drawbacks of this process, see Chapter 5

[72] For an interesting discussion on the interpretation of the UK law in using PII for medical research, see Walley T (2006) 'Using personal health information in medical research: Overzealous interpretation of UK laws is stifling epidemiological research' in BMJ January 2006 21; 332(7534): 130–131

- PII in the context of the 1998 Act is 'personal data' which is defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly'
- 'Identifiability' is crucial to the law. If an individual is not identifiable, e.g. following anonymisation, then the DPA does not apply to the processing of the anonymised data. Note, however, that the person who performs the anonymisation and who can re-identify the individual remains subject to the DPA requirements.
- What counts as the processing of PII? The term 'processing' covers almost every imaginable form of dealing with data, including collection, organisation, adaptation, retrieval, consultation, disclosure, combination and blocking of data and the process of anonymisation.
- Who is the data controller and in what circumstances does this role arise (especially in light of inter-institutional exchanges of data)? Section 1(1) DPA defines the data controller (DC) as 'a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'. Thus there can be multiple data controllers in any given data exchange.
- Who is responsible when data are moved between different entities, where the data may become PII when linked? This is one question which lacks a clear answer; things become especially complicated where data are shared between different countries, particularly sharing between EEA (European Economic Area) and non-EEA countries where data protection standards may be different.[73]

- The Article 29 Working Party suggests that where diverse actors are involved in data transfer and processing, ' one should avoid a chain of (sub-)processors that would dilute or even prevent effective control and clear responsibility for

[7373] The difference between safe harbours and safe countries should be noted. The safe harbour framework is designed to facilitate data exchange between organizations in the USA and EU countries. The EU Commission certifies that certain US organisations have fulfilled EU DP Directive 'adequacy requirements' i.e. that they share the same data standards as EU countries, and EU member states will be bound to respect this finding of adequacy when considering whether or not to share data with the US organisations. Medical data in the USA is often handled by non-governmental organisations, thus bypassing safe harbour requirements.

processing activities, unless the responsibilities of the various parties in the chain are clearly established'.[74]

1) Who is responsible?

The data controller, this is a natural or legal person who 'alone or jointly with others determines the purposes and means of the processing of personal data' [75]

2) For what?

For ensuring compliance with the Data Protection Principles for example that data are processed lawfully and fairly, that linked data sets are kept no longer than necessary and that no more personal information than completely necessary is used.

3) What are the penalties?

Under s60 (2) DPA, individuals guilty of committing offences under the Act may be liable to pay monetary fines. Further, s 60(4) stipulates that the court 'may order any document or other material used in connection with the processing of personal data and appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.'[76]

Section 77 of the Criminal Justice and Immigration Act 2008 provides that those breaching s 55 DPA (obtaining or disclosing personal information without consent from the data controller) may be subject to penalties of up to 2 years custodial sentencing. Note that before the courts hand out such penalties, the Information Commissioner must be consulted.

4) What are the flexibilities?

Exemptions include where information was obtained, disclosed/procured in the prevention of crime, authorised by law, where the individual believed he would have the right in law to obtain the information/the consent of the DC, where this was justified in the public interest.[77]

[74] Article 29 Data Protection Working Party (2010) Opinion 1/2010 on the concepts of "controller" and "processor" see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf
[75] European Data Protection Directive
[76] Section 60 (4) Data Protection Act 1998
[77] See s55(2) DPA 1998

The research exemption under s.33 allows special provisions to be made where certain criteria are fulfilled e.g. 'the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them, the data are not processed to support measures or decisions with respect to particular individuals' etc. Section 33 gives relief from subject access rights and data retention requirements and offers quite useful exemptions in the research context. However, data subjects should still be made aware of the fact that their data may be processed for research purposes in the future. It should also be noted that the DPA does not apply to the deceased.

5) What is the role of consent, anonymisation and authorisation?

Although consent is a sufficient mechanism to process data, it is not absolutely necessary; moreover, simply because consent has been obtained does not absolve the DC and data processor from wider obligations under the Act e.g. fair and lawful processing, informing people about data uses etc.

Regarding anonymity, the DPA ceases to apply.

On authorisation, there is no specific provision but any authorising body would clearly have to comply with data protection principles, this is the case for the Ethics and Confidentiality Committee (ECC) which is constrained both by DPA and HRA.

The Caldicott Principles

The Department of Health Caldicott Committee Report in 1997 (Caldicott Report) laid out six key principles[78] that must be taken into consideration when handling data, the principles relate not only to the use of PII for treatment, but also for research purposes[79]. The principles are:

- justification of purpose
- don't use patient information unless absolutely necessary

[78] This set of principles was adopted in Scotland by NHS MEL (1999) 19 Caldicott Guardians http://www.sehd.scot.nhs.uk/mwls/1999_19.doc

[79] 'Guidance must be provided for those individuals/bodies responsible for approving uses of personally-identifiable information (for example. the "guardian" or research ethics committees) to enable them to critically appraise new proposals and continuing practice.' – Department of Health, The Caldicott Committee, 'Report on the Review of Patient-Identifiable Information' 1997, para 4.4.3 (p19)

- use the minimum information necessary
- access should be on a strict need-to-know basis
- be aware of your data handling responsibilities
- understand and comply with the law

1) Who is responsible?

The Caldicott Guardian (see below at page 60 for a more detailed description of this role)

2) What for?

For ensuring an understanding of and adherence to the Caldicott Principles by all individuals handling PII.

3) What are the penalties?

Those relating to a breach of the common law duty of confidentiality. In Scotland, this would involve an interdict in order to stop the PII from being disclosed and/ an award of damages.

4) What are the flexibilities?

The Caldicott Guardian is quite a powerful actor (see page 60)

5) What is the role of consent, anonymisation and authorisation?

The Caldicott Guardian is principally concerned with authorisation.

The CG could insist that consent is obtained from individuals before their PII is used and/or that the data undergo anonymisation.

The common law duty of confidentiality

In addition to satisfying the DPA 1998 requirements, those dealing with PII must also act in compliance with the common law duty of confidentiality whereby there exists a duty not to disclose confidential patient information. However, legitimate justifications for disclosing such information exist, including where consent has been obtained and

where disclosure is in the public interest or where there is a legal requirement e.g. public health legislative requirement to notify a particular disease.[80]

It should be noted that the concept of public interest as a justification is wide, and 'there are areas which have not been litigated, where it is impossible to state with any certainty whether a duty of confidence exists and, therefore, that the consent of patients is required for the processing of their data. Even where there is case law, it may be difficult to extrapolate general principles from the particular circumstances of the case. There is no certainty that a decision made many years ago by a court would be reflected in a decision made in the context of a modern NHS.'[81]

Confidentiality is also a cornerstone of medical ethics and a key element in medical professional guidance. Thus, it may be more appropriate to refer for example to GMC (General Medical Council) Confidentiality (2009)[82] which offers guidance on principles of confidentiality and privacy for doctors.

1) Who is responsible?

All individuals handling PII.

2) For what?

Maintaining the duty of confidentiality under which they are obliged not to disclose confidential patient information without consent or without a legitimising basis.

3) What are the penalties?

The responsible party may be liable to pay the patient damages for the breach. In contrast to the DPA, the duty of confidentiality does apply to the deceased. GPs in particular might face professional standard repercussions for example, disciplinary action from the GMC or even losing their licences for serious breaches.

[80] Another example is the reporting (anonymously) of abortion statistics.
[81] Information Commissioner's Office (2002) see n36
[82] GMC Confidentiality Guidance (2009) view report at - http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_contents.asp

4) What are the flexibilities?

Individuals will avoid liability where the patient has given consent for the disclosure, where the individual can demonstrate that disclosure was based on an 'overriding' or 'substantial' public interest or where there is a legal duty to disclose the information

5) What is the role of consent, anonymisation and authorisation?

Consent plays a key role here as its presence frees up individuals from liability.

Suitably anonymised data is arguably no longer confidential as its use or disclosure cannot harm any particular individual.[83]]

A Caldicott Guardian can authorise the use of confidential information but this might not absolve a user of legal liability if they Guardian has acted outside his or her authority.

The NHS Act 2006

In England, section 251 of the NHS Act 2006[84] allows the common law duty of confidentiality to be set aside by the Secretary of State for Health in those instances where PII is required for medical purposes (including medical research). Such action must be justified in the public interest, where neither anonymisation of data nor obtaining patient consent is practicable (having regard to the cost and technology available).[85] Further, the ECC (Ethics and Confidentiality Committee) must be consulted in order to obtain authorisation.[86] It is interesting to note that the Patient Information Advisory Group (PIAG, and the forerunner to ECC) was initially set up as a temporary measure and it was intended that the group be abolished once consent/anonymisation/pseudonymisation was adequately achieved.

[83] R v Secretary of State for *Health*, *ex parte Source Informatics*, [2002] QB 424 CA

[84] Formerly Section 60 of the Health and Social Care Act 2001

[85] Wellcome Trust (2009) Report - 'Towards Consensus for best practice - use of patient records from general practice for research' accessible at http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtx055660.pdf

[86] The ECC operates under the auspices of the NIGB (National Information Governance Board for Health and Social Care) and enjoys delegated powers from the NIGB (see s.251 NHS Act 2006).

Scotland does not enjoy a statutory equivalent to section 251, however, in NSS, its Privacy Advisory Committee (PAC) serves a similar purpose in advising on requests where consent has not been obtained for (1) PII and (2) linkages in relation to datasets of which it is custodian which could lead to identifiability of data subjects, PAC is discussed further below. It is also worth noting that while PAC exists, reliance is still put either on implied consent or on the public interest justification, which remains a vague concept given the lack of case law in this area.

Key message

- Is the absence of legislation permitting the overriding of the common law duty of confidentiality for specific controlled health-related issues (including research) a hurdle? Should Scotland consider the creation of a statutory body similar to the ECC?

1) Who is responsible?

Doctors and all healthcare professionals and NHS staff and contractors dealing with PII, ECC and PAC.

2) For what?

Upholding their obligations of confidentiality under the common law.

3) What are the penalties?

Those related to the common law action of breach of confidence. Mainly, penalties will involve either an interdict to stop the confidential information from being disclosed, or, an award of damages.

4) What are the flexibilities?

In England, the common law duty can be set aside where justified in the public interest and in Scotland, PAC serves a similar purpose although there is no means to set aside legal obligations. No protection is therefore given to researchers or other users/data handlers in light of a recommendation from PAC.

5) What is the role of consent, anonymisation and authorisation?

The key role played is of providing authorisation for the use of PII. This mechanism is specifically deployed when consent and anonymisation are impossible, impracticable or fail to strike an appropriate balance between public interests.

The Freedom of Information (Scotland) Act 2002 (FOISA)

Scotland adopted the Freedom of Information (Scotland) Act in 2002[87] which offers similar provisions to the Freedom of Information 2000 Act[88] which applies in England and Wales. This Act sets out to promote openness and accountability for public information held by public authorities. It provides that subject to exceptions, upon request, a public authority, must disclose public information[89] which they hold. Public information refers to information held by public authorities under the Freedom of Information Act**.**

Key Message -

- A public authority does not have to disclose information on data it holds about identifiable individuals as identified in the DPA. The relationship between DPA and FOISA remains unclear in certain aspects, at least following the Collie case, we know that DPA trumps FOISA.[90] Clarification of the Collie case (CSA V SIC)[91]was widely anticipated because it was hoped that it would help us to understand what constitutes adequate anonymisation in law i.e. when are statistical/aggregated outputs personal data and their release potentially in breach of the DPA Principles. In Collie, the Scottish Information Commissioner

[87] For more information on how the Scottish Government supports the freedom of information, see Scottish Government 'Freedom of Information - the Scottish Government's Six Principles' at http://www.scotland.gov.uk/About/FOI/6principles/Q/EditMode/on/ForceUpdate/on

[88] However, differences do exist between the Acts, for example, in the UK, an Information Tribunal exists, allowing those opposing decisions of the Information Commissioner to appeal them, no such Tribunal exists in Scotland.
For a detailed account of differences between the Freedom of Information 2000 and the Freedom of Information (Scotland) Act 2002, see 'Freedom of Information (Scotland) Act 2002 - A guide for the Information Professional' at http://www.slainte.org.uk/files/pdf/foi/foisa04.pdf

[89] Such requests are commonly referred to as 'FOIs'

[90] For an interesting analysis of the relationship between FOIA and DPA, see Laurie G and Gertz R (2009) 'The Worst of All Worlds? Common Services Agency v Scottish Information Commissioner' in EdinLR Vol 13 pp 330-334

[91] This case involved Michael Collie who submitted a FOI Request to the Common Services Agency (CSA), part of the NHS, information on childhood leukaemia data for the Dumfries and Galloway area of Scotland was requested. The CSA refused to satisfy the request, arguing that the information could allow the identification of patients. After hearings in the Scottish Courts and the House of Lords, we await clarification from the Scottish Information Commissioner on the relationship between the DPA and FOIA.

acknowledged that Mr Collie's information request was exempt under section 38(1)(b) FOISA due to the sensitive nature of the statistics requested and that disclosure of this information would constitute a breach of the first DPA Principle. However, he also acknowledged that duty imposed on the CSA under FOISA section 1(1) to provide statistical information to Mr Collie 'in a form which would not lead to the identification of the individuals in question, when such disclosure was possible. The Commissioner has agreed with the CSA the form in which this information should be disclosed'.[92]

1) Who is responsible?

Public authorities, including NHS entities such as NSS (National Services Scotland) and Health Boards. This includes NHS ISD (the Information Statistics Division), which is the leading custodian on health statistics and statistical disclosure control measures to safeguard privacy.

2) For what?

Ensuring compliance with FOIA, including responding to FOI requests within the specified period of time. For example, requests regarding linkages taking place, data sets which ISD holds may be made.

3) What are the penalties?

Currently, no right of monetary compensation from a public authority in breach of their statutory duties exists, however an enforcement notice may be served requiring the public authority to satisfy the FOI request when it has previously declined to do so. See below for discussion on imminent increase in powers.

4) What are the flexibilities?

There are some circumstances in which a body does not have to disclose information. These include where information can be defined as 'personal data' under the DPA,

[92]Decision 021/2005 Mr Michael Collie and the Common Services Agency for the Scottish Health Service accessible at http://www.itspublicknowledge.info/applicationsanddecisions/Decisions/2005/200500298.asp

where it is readily available from an alternative source, national security exemptions, information in court records etc, for a full list refer to FOIA 2000 s 21-44[93]

5) What is the role of consent, authorisation and anonymisation?

The key role here is of authorisation, that is, where public authorities agree to disclose information in response to FOI requests. As noted above however, the roles of consent, authorisation and anonymisation may be clarified once light is shed on the relationship between the FOIA and DPA.

Interim conclusion on legal provisions relating to information governance

- The EU Data Protection Directive governs the processing of PII within the EEA however Member States enjoy some discretion in how they interpret the Directive. This Directive was incorporated into UK law as the Data Protection Act 1998
- The DPA 1998 identifies the data controller as the key entity responsible under this law.
- Under Article 8 HRA 1998, respect for private life must be observed; this right is not absolute, and should be balanced with the interests of others. Any departure from the right must be justified in the names or the rights and freedoms of others and as necessary and proportionate.
- The common law duty of confidentiality imposes an obligation not to disclose confidential patient information; however this can be set aside where disclosure is in the public interest. 'Public interest' is however, an uncertain concept upon which to rely because it has never been tested in court in the medical research context.
- Under s251 NHS Act 2006, the common law duty of confidentiality can be set aside in the public interest in England by an Ethics and Confidentiality Committee (ECC).
- No such legislation exists in Scotland.

[93] For Scotland, see Freedom of Information (Scotland) Act 2002

- In relation to those data under the custodianship of NSS, the Privacy Advisory Committee (PAC) authorises the use of PII where consent has not been obtained.
- Public authorities must disclose public information held by them but this does not extent to personal data as defined by the Data Protection Act 1998.

4.2 Key formal actors

We choose to use the second stage of our scoping exercise to 'establish and explore the power, status, roles and interrelationships of the regulatory actors with "formal" authority'[94] to regulate medical research.

While for the most part, regulation of data protection for PII will be on the national level, we must remember that certain European bodies exert considerable influence in this area. However at times guidance from differing bodies can be conflicting, thus, as Kaye and Gibbons put it, 'this raises difficult questions over their rank and relationship'.[95] Main European actors whose presence must be noted include the European Institutions i.e. Commission, Parliament and Council of Ministers (this is supported by Parliament's EU Data Protection Directive and the Council of Ministers' recommendation'), the Council of Europe and the European Data Protection Supervisor (EDPS) who 'is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies' [96].The EDPS offers advice on legislation and policies that may affect privacy and is committed to ensuring data protection standards are parallel throughout the EEA. Directives play an important role in EU law in that the Member States concerned are obliged to implement the changes stipulated by the Directives. Whilst Recommendations are not

[94] With thanks to Kaye and Gibbons (2008) at 117.
[95] Ibid
[96] European Data Protection Supervisor, 'The European Guardian of Personal Data Protection' accessed at http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

binding, they can be influential in political terms, in that national courts should interpret legislation in accordance with the recommendations.[97]

The European DP Directive also established the Article 29 Data Protection Working Party consisting of one representative of the data protection authority for each Member State. The working party provides the Commission with advice regarding questions of data protection and of how individuals' rights with regard to data protection and privacy may be affected by Community measures; it also issues recommendations on such matters.[98]Although its opinions are not binding, they can be very persuasive regarding the way in which national courts interpret data protection law. For example, Opinion 4/2007 on the concept of personal data offers a helpful analysis of the meaning of the definition of personal data in the EU DP Directive and the Working Document on Genetic Data (2004). In particular, the Working Paper on electronic health records (2007) sets out helpful guidance on how the data protection rights or patients should be respected as well as information on data sharing and international transfer of medical records. The working party has recently administered guidance on the subsequent roles of data controllers and data processors (as discussed at page 43) in addition to its most recent Opinion on Consent (2011) (discussed at page 14)[99]

Information Commissioner's Office (ICO) UK

1) What governance role do they play?

The ICO is responsible for overseeing and enforcing the DPA and FOIA.[100] The public body is charged with promoting compliance with DPA requirements, as well as delivering rulings on complaints for breaches of the relevant legislation and prosecuting those who are found to have committed breaches, in addition to maintaining a register of data controllers in the UK.

2) By what authority do they play this role?

[97] Fairhurst J and Vincenzi C (2003), 'Law of the European Community' (4th Ed.), Pearson/Longman, London, p. 41 at 396

[98] Further information including a list of all documents released by the Working Party can be accessed at the European Commission website at - http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[99] Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent

[100] The ICO also oversees compliance with the Environmental Information Regulations and the Privacy and Electronic Communication Regulations. For more information on the ICO, see – http://www.ico.gov.uk/about_us.aspx

The ICO is sponsored by the Ministry of Justice, set up as an Independent UK Authority.

3) What sanctions apply?

To present, the ICO has relied heavily on voluntary compliance and has been accused of lacking the necessary powers of enforcement, commonly referred to as its 'toothlessness'. However, it was recently awarded powers to enforce monetary fines of up to £500,000 for data security breaches, thus providing a substantial deterrent against data breaches.

4) How effective are they as data gate-keepers?

The ICO plays an important role in promoting DPA compliance; it offers a wide array of guidance on DP issues for organisations and the public, including helpful publications and guides for example, on performing PIAs.

Scottish ICO

1) What role do they play?

While the UK ICO is responsible for DPA, Freedom of Information Act, Environmental Information Regs, Privacy and Electronic Communications Reg, the regional office of the Scottish Information Commissioner is responsible for public authorities carrying out devolved acts, particularly those concerning the Freedom of Information (Scotland) Act 2002

2) By what authority do they play this role?

Again, the Scottish ICO is nominated by Scottish Parliament, in the UK, the ICO is sponsored by the Ministry of Justice.

3) What sanctions apply?

Current powers with respect to the Freedom of Information Act include the ability to 'serve an information notice on a public authority requesting further information in relation to the matter. The Scottish Commissioner also has the power to negotiate between both parties in an attempt to effect settlement. In certain circumstances, the

Scottish Commissioner may issue a decision or enforcement notice requiring disclosure of information in the public interest.'[101]

4) How effective are they as data gate-keepers?

Similarly to the ICO, the Scottish ICO has considerable weight in influencing practices amongst organisations handling PII. A key challenge however, has been the complicated relationship between FOI (which promotes a culture of openness) and the DPA (which is centred on maintaining privacy of PII). Such complexities were highlighted by the Collie Case[102] where an FOI request regarding childhood leukaemia in Dumfries and Galloway made to the Common Services Agency (CSA) was refused on the basis that the information could allow the identification of patients. As stated above, after hearings in the Scottish Courts and the House of Lords, the Scottish Information Commissioner has opined that whilst the CSA were correct in not disclosing sensitive personal data in accordance with the first Data Protection Principle, they were obliged under the FOISA to provide the statistical information in an alternative form which would not allow for the identification of data subjects. The SIC has subsequently agreed with CSA on an acceptable form in which the data can be disclosed.[103]

Caldicott Guardians (CGs)

Key Messages

- Many individuals are unaware of who their local CG is
- Those dealing with requests to share data with researchers are unsure as to whether it is they or the CG who would be held liable in the case of misuse of the data
- Can/should GPs be seen as data controllers under the DPA? Yes that has been the NHS policy position for some time; the GP partnership or, equally, single-handed practitioner is a data controller which must register its processing with ICO and abide by the DP Principles etc. A member of Practice staff e.g. Practice manager

[101] JISC, 'Freedom of Information Act 2002: Implementation and Practice (Scotland) at http://www.jisc.ac.uk/publications/documents/pub_ib_fois.aspx#05enforcement
[102] Common Services Agency v Scottish Information Commissioner [2008] 1 WLR 1550
[103] http://www.itspublicknowledge.info/applicationsanddecisions/Decisions/2005/200500298.asp

will look after the Data Protection register entry etc and a medical practitioner will be asked to lead/advise on confidentiality/Caldicott matters.

1) What governance role do they play?

In addition to the six Caldicott Principles, the Caldicott Report stipulated that all NHS organisations which deal with personal data should appoint Caldicott Guardians (CGs). These individuals are responsible 'for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing'[104]. CGs should preferably be 'at Board level, be a senior health professional and have responsibility for promoting clinical governance within the organisation'[105], as the NHS puts it, they are 'the conscience of an organisation'.[106]

Ensuring adherence to the Six Caldicott Principles (see above): 'The main concerns of the Caldicott Guardian will be the protection of personally identifiable information from unlawful and unethical disclosure; and the facilitation of information sharing without the use of such data.'[107]

2) By what authority do they play this role?

In England, CGs are appointed by chief-executives of NHS organisations 'each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012. The mandate covers all organizations that have access to patient records, so it includes acute trusts, ambulance trusts, mental health trusts, primary care trusts, strategic health authorities, and special health authorities such as NHS Direct'[108]

[104] Department of Health website ' 'NHS Caldicott Guardians' http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563

[105] Caldicott Guardian Circular for CGs in England http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4011935.pdf

[106] NHS Connecting for Health, 'Caldicott Guardians' - http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

[107] NHS 'Caldicott:Principles into Practice', see http://www.wales.nhs.uk/sites3/page.cfm?orgId=783&pid=31174

[108] NHS Connecting For Health see n79

Similarly, in Scotland, CGs were introduced via MEL (1999) 19, however here, CGs are appointed by Health Boards, and this included nominating CGs not only at Board level, but also in 'other organisations who share NHS patient information, such as the divisions of the CSA who hold patient identifiable information, the Scottish Centre for Infection and Environmental Health (SCIEH), Universities and Research Bodies, Mental Welfare Commission'.[109] A Caldicott Guardians Forum now exists in Scotland.

3) What sanctions apply?

Those penalties related to the common law duty of confidentiality, in Scotland this means either an interdict stopping use of the PII and or an award of damages to the data subject.

4) How effective are they as data gate-keepers?

CGs play a large role in ensuring that PII is handled in the appropriate manner, this includes determining whether to allow the sharing or withholding of PII.

This being said, the CG role is limited in the sense that GPs are the data controllers of the personal health information their patients trust them with. GPs may take advice from their appointed CG if they are aware of whom this individual is. Alternatively, GPs take advice on these matters from their (often conservative) defence unions.

Authorising bodies

This section looks at the role of authorising bodies in the governance of PII. Here, we are not only dealing with Research Ethics Committees (RECs), but also, advisory bodies such as the Privacy Advisory Committee (PAC) in Scotland which, as we have seen, holds no statutory powers.

Key Messages

- Authorising bodies carry considerable weight in the governance of PII however are often lacking in statutory powers.

[109] NHS MEL 19 (1999) Caldicott Guardians in Scotland, see http://www.show.scot.nhs.uk/Publications/index.asp?offset=2884

- Key questions here are - when is it necessary to obtain approval from an ethics committee for research involving PII? When this PII has been obtained without the consent of data the data subjects and the data will not be anonymised?
- There is a need for clarity of function between bodies and a need to reduce confusion regarding their respective remits and any overlap which exists.

1) What governance role do they play?

It is for authorising bodies, commonly in the form of research ethics committees (RECs) to 'safeguard the rights, safety, dignity and well-being of people participating in research in the National Health Service.'[110]

Whilst authorising bodies do not always enjoy legal authority, they do, nonetheless, play an important role in the governance of personal data for medical research and decisions taken by them can be subject to judicial review.

2) By what authority do they play this role?

Despite the importance of their role, the power enjoyed by such authorising bodies should not be overestimated, 'because RECs lack formal powers, a necessary quid pro quo is that those other agencies must provide the missing backbone'.[111] 'Those 'other agencies' relate to, for example, the NHS, the GMC and in particular funding bodies who make pre-approval by RECs a necessary condition to their disclosure of PII/award of funding.[112]

England - Under the auspices of the National Information Governance Board for Health and Social Care (NIGB), the Ethics and Confidentiality Committee[113] (ECC) is charged with offering advice on and considering ethical issues arising from the processing of information relating to health and social care. It consists of 16 members, meeting bi-monthly. It authorises the use of PII without consent under its delegated powers.

[110] NHS National Research Ethics Service, 'The role of RECs' accessible at http://www.nres.npsa.nhs.uk/aboutus/about-recs/role-of-recs/

[111] Kaye and Gibbons (2008)

[112] ibid

[113] Before this committee was established, a similar role way played by the Patient Information Advisory Group

Further, by virtue of section 251 of the NHS Act 2006, the ECC is responsible for considering applications requesting permission to use section 251 in setting aside the common law rules of confidentiality.[114] This serves to protect those bodies which disclose such identifiable information from legal actions for having breached confidentiality.

3) What sanctions apply?

'NHS employees failing to seek approval from the relevant REC are likely to be disciplined by their employing trusts. Outside the NHS, researchers may face disciplinary action by professional regulatory authorities. Conducting research without ethical review may constitute impaired "fitness to practise"'.[115]

Those subject to s251 penalties may be subject to a fine or 'other procedures for enforcing any provisions of the regulations'.[116]

Where permission to use section 251 NHS Act 2006 to set aside the common law duty of confidentiality has not been obtained from the ECC, individuals may face penalties under the common law for breach of confidentiality, which can involve paying damages.

4) How effective are they as data gate-keepers?

It is interesting to note that neither NIGB nor the ECC have been endowed with statutory authority from the Secretary of State but rather they act in an advisory capacity. Although their powers thus appear limited, they are, in fact quite extensive if we consider that the ECC has been delegated the responsibility of administering s251 powers from the NIGB and, that the Secretary of State is compelled, under s251, to consult the NIGB prior to laying any revised regulations before Parliament. This is a perfect illustration of why such regulatory space exercises are so useful, they allow us to reveal key actors who possess more power than envisaged at first glance. Further, this reminds us that a wealth of power rests in actors who are not necessarily endowed with legal powers.[117]

[114] This is discussed earlier when explaining legislation and obligations under statute

[115] Brazier M, Cave E (2007)' Medicine, patients and the law' 4th Edition London: Penguin,

[116] NHS (2006) Act s251 (2)(d)

[117] The Database Monitoring sub-Group (DMsG) operates under the ECC, its role is 'to review applications relating to Hospital Episode Statistics and Central Register data, which were previously reviewed by the Security and Confidentiality Advisory Group (SCAG) or the Office of National Statistics Advisory Group for Medical Research.' See NIGB, 'Database Monitoring Sub-group' see http://www.nigb.nhs.uk/ecc/dmsg

Scotland

PAC (Privacy Advisory Committee)

Key Messages

- There is a lack of clarity about the precise remit of PAC
- There is a lack of clarity about the nature of the relationships between ethics committees and other authorising bodies such as PAC.
- Should a greater role be envisaged for PAC?
- To what extent is the ECC (Ethics and Confidentiality Committee) a model that PAC or a body similar to PAC could/should follow?

1) What governance role do they play?

In Scotland, responsibilities as exercised by the ECC are carried out by a similar but smaller body, the Privacy Advisory Committee (PAC) which deals with requests for the use of person identifiable information from the Information and Statistics Division (ISD) or NRS (National Records of Scotland). However, it is important to note the difference between the ECC which authorises use of PII and PAC which is limited to acting in an advisory capacity to ISD and NRS and it does not provide official advice: 'When wishing to use Scottish Morbidity Records (SMRs) for medical research studies, involving release of information by ISD from which patients can be identified and/or linkage of previously unlinked records; then an application must be submitted to the PAC.'[118]

PAC meets only twice a year however it transacts the majority of its business in between meetings via (e)mail. It consists of 5 official members.

2) By what authority do they play this role?

PAC currently lacks a statutory basis and thus its capacity is limited to offering advice as opposed to authorisation.

3) What sanctions apply?

[118] MRC Data and Tissues Tool Kit, 'Seeking Approvals: Privacy Advisory Committees' http://www.dt-toolkit.ac.uk/routemaps/station.cfm?current_station_id=430

As mentioned above, researchers and NHS employees alike would likely face disciplinary action and particularly for researchers, withdrawal/refusal of funding applications.

4) How effective are they as data gate-keepers?

Despite the lack of statutory power, PAC plays a key role in Scotland regarding the use of PII for medical research. For example, ISD/NRS internal procedures would not allow the use of PII without prior consideration by PAC or a decision by the CG, funding bodies are also unlikely to invest in any research project which has not received prior PAC approval.

The remit of PAC does not extend to the data held by Health Boards or GPs or indeed any other body outside the purview of ISD or NRS. Linkages and sharing must therefore be negotiated and agreed between the respective data controllers.

The General Medical Council (GMC)

1) What governance role does it play?

Amongst its various roles, the GMC aims to promote good medical practice as an independent regulator for doctors; it issues guidance on many aspects of practice, including confidentiality. The most recent GMC guidance on confidentiality advises doctors that '[w]hen disclosing information about a patient, you must use anonymised or coded information if practicable and if it will serve the purpose'.[119]

Further, it has advised that consent should be obtained prior to disclosure of information for medical research. It states that when dealing with disclosure of PII for research, 'in considering whether it is practicable to seek consent you must take account of:

(a) the age of records and the likely traceability of patients

(b) the number of records, and

(c) the possibility of introducing bias because of low response rates or because particular groups of patients refuse, or do not respond to, requests to use their information.

[119] GMC, 'Confidentiality Guidance' Oct 2009

Further, a range of factors for consideration of whether the interest in maintaining confidentiality is outweighed by the public interest in disclosing PII for research are provided. Namely; ' the nature of the information to be disclosed, what use will be made of the information, how many people will have access to the information, the confidentiality and security arrangements in place to protect the information from further disclosure, the advice of a Caldicott Guardian or similar expert adviser, who is not directly connected with the use for which disclosure is being considered, and the potential for distress or harm to patients'[120].

2) By what authority does it play this role?

The GMC was established under The Medical Act of 1858. Subsequent legislation relating to its roles and powers include The Medical Act 1983 (including the most recent 2006 amendments) and Directive 2005/36/EC on the recognition of professional qualifications.[121]

3) What sanctions apply?

As an Independent Regulator, the GMC is accountable to the public for its actions. In turn, its powers include the right to withdraw licences from medical practitioners who fail to uphold their professional obligations, in our context, this would of course relate most directly to maintaining dr-patient confidentiality of personal information, unless consent for disclosure was granted by the patient.

4) How effective are they as data gate-keepers?

The GMC is most influential as a data gate-keeper amongst medical practitioners because it has the power to revoke licences where dr-patient confidentiality is breached, thus the guidance if offers on confidentiality matters carries considerable weight when doctors are handling PII and considering sharing it.

The Information Statistics Division (ISD)

1) What governance role does it play?

[120] ibid, pgph 44.
[121] GMC, About us - Legislation, see http://www.gmc-uk.org/about/legislation.asp

Information Services Division (ISD) of NHS National Services Scotland acts as the custodian of NHS Scottish Morbidity Records (SMR) Datasets in Scotland. It deals with requests from researchers who wish to gain access to data stored at ISD. However, it is NSS – the body under whose auspices ISD operates - which acts as a DC. It is also charged with the collection and dissemination of epidemiological data and participating in epidemiological investigations.[122]

2) By what authority does it play this role?

It operates as 'a business operating unit'[123] of NHS National Services Scotland

3) What sanctions apply?

NSS (on behalf of ISD) is subject to the same penalties as any other DC.

Internally, for NHS Scotland employees working at ISD, adherence with the Confidentiality Guidance which is supplied to staff is necessary. The guidance covers all aspects of DP issues, including, importantly in this context, types of data which can and cannot be communicated.

Staff are required to sign a confidentiality guidance document once a year, which represents their agreement to comply with the DP standards expected, where non-compliance is practiced, staff risk disciplinary action or even losing their jobs.

Outside of ISD, where data sharing occurs, ISD demands that data recipients report any inappropriate use of the data to a Caldicott Guardian or directly to ISD where an incident report is made however NHS Info Security Policy does not necessarily say that entities to which data are sent must comply with the same level of security as within NHS Scotland.

It is suggested that ISD relies more on a strong desire to uphold a good reputation, both from their own part, and the part of those requesting data than a hard-lined approach to ensuring compliance. After all, the wealth of data available is so valuable to researchers and the public interest in good medical research is stressed here. Scotland is relatively

[122] These responsibilities are by virtue of the National Health Services (Functions of the Common Services Agency) (Scotland) Order 2008 section 2(j).

[123] NHS NSS, ISD Scotland, 'Our Organisation' accessed at http://www.isdscotland.org/isd/3352.html

small in that where a reputation for good DP standards is tarnished; this itself may impede access to data substantially.

4) How effective are they as data gate-keepers?

As data custodian for all NHSS SMR datasets, ISD plays a considerable role in providing or denying access to rich data sets. SHIS-R (the Scottish Health Information Service for Research) will act as a portal for facilitating large scale linkage of data sets between ISD and third party data sets thus internal governance mechanisms will play an important role not only for medical research but for research based on linkages between health and non-health data as has ultimate say over who can access the data.

4.3 Informal actors - 'beyond the formal structure'

Funding Bodies

1) What governance role do they play?

Although funding bodies such as the Wellcome Trust are not legal actors per se, the influence which they can exert is considerable, particularly where projects may compromise the reputation/go against the best practice of the particular source of funding. Often, such funding bodies have their own policies and consultation papers, for example, the Wellcome Trust has its 'Policy on the use of personal information in research', 'Guidelines on good research practice', 'Policy on data management and sharing' and a consultation response on 'Use and sharing of personal information in the public and private sectors'.[124]

2) By what authority do they play this role?

Their authority/power is gained through obligations they place upon researchers to obtain funding in a competitive environment; they make confidentiality and other matters a condition of awarding grants.

3) What sanctions apply?

[124] These policies and papers can be accessed at - http://www.wellcome.ac.uk/About-us/Policy/Spotlight-issues/Personal-information/Policiesandpositions/index.htm

No funding body desires to be affiliated with research which has been carried out in breach of fundamental laws or ethical principles. For example, in light of a 2008 publication which highlighted that *'it was possible to identify individuals whose genomic data had been included in a cohort of anonymised genetic profiles made available to researchers over the internet'*, both the Wellcome Trust and the US National Institutes of Health abandoned their systems of open data sharing among researchers.[125]

4.4 Problems with the current landscape

The Academy of Medical Sciences published an informative report in 2006 entitled 'Personal data for public good: using health information in medical research', in which it identified several perceived problems with the current governance structures in England and Wales, however many matters discussed also apply to Scotland.

In addition to highlighting confusing legislation and guidelines, it criticised the current landscape for over emphasising privacy and autonomy at the expense of public benefit. Further, it argues that a 'culture of conservative governance' has emerged where inadequate public engagement has led regulators and advisory bodies to making judgements on behalf of the public as to what they would find (un)acceptable regarding use of their PII. Thus, it is argued, 'disproportionate constraints lead to the compromise of the quality and validity'.[126] Similar themes were raised in the Academy's 2011 report 'A new pathway for the regulation and governance of health research'.

Sensitivity to a wide range of stakeholders' interests and a need for a governance framework that is fit for purpose over time are necessary considerations. Moreover, it is essential to engage with stakeholders throughout the construction and implementation of a governance framework in order to understand these interests and how they might evolve over time. The Public Engagement stream of SHIP is involved with researcher, patient and healthcare professional focus groups for this purpose. The failure to have robust engagement mechanisms relating to the present system brings its fitness for purpose immediately into question.

[125] Homer et al (2008) 'Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping micro arrays' in Public Library of Science Genetics J 4:e1000167.
[126] The Academy of Medical Sciences, 'Personal Data for public good: using health information in medical research' (2006)

It is also open to question whether PAC needs to be more formalised and legally constituted because at present, it lacks a formal legal basis for its existence as well as formal powers. However, NSS has a statutory authority and is free to establish an advisory committee to advise it in its work.[127] A broader question is whether a PAC-like body is need in Scotland which could assume similar roles but for a broader range of data controllers and with a clearer remit and sense of purpose.

Research Ethics Committees rely heavily on other bodies to ensure compliance, thus there is always the danger that 'other agencies might decline to respond to the ethical violations'.[128] Further, as REC approvals 'rest on proposed not actual protocols for running specific projects, once projects are up and running, RECs may lack monitoring ability'.[129] However, concerning NHS studies, it should be noted that where RECs fail to intervene, NHS R & D (Research and Development) will take on the responsibility of monitoring for compliance and misdemeanours might result in withdrawal of approval whereby study results cannot be published or indemnity insurance might be lost.

It is not possible always to limit the use of PII for research to the original purpose for which consent was obtained, thus those involved are often required to consider obtaining consent for the new purpose. Where obtaining consent is not possible/feasible, the PII must be anonymised/pseudonymised. Further, according to DPA 1998, each time that a patient record is processed, the necessity test must be fulfilled.

The 'consent or anonymise' approach does not always work, as discussed by the Academy of Medical Sciences. This approach not only adds financial and labour intensive burdens on those requesting permission to use the data, but the process of anonymisation/pseudonymisation has the potential to diminish the richness or value of certain datasets[130].

[127] The National Health Services (Functions of the Common Services Agency)(Scotland)Order 2008
[128] Kaye and Gibbons (2008) at 121 see n2
[129] ibid
[130] The Academy of Medical Sciences, 'Personal data for public good: using health information in medical research' (2006)

Along with the lack of clarity in the law, (in our knowledge), the courts have not tested PII breaches in specific context of medical research[131], thus adding more uncertainty as to how such a breach would be treated.

In their 'Data Sharing Review Report'[132], Walport and Thomas highlight the lack of clarity in legislation governing data sharing and data protection -

'the Data Protection Act fails to provide clarity over whether personal information may or may not be shared. The Act is often misunderstood and considerable confusion surrounds the wider legal framework – in particular, the interplay between the DPA and other domestic and international strands of law relating to personal information. Misunderstandings and confusion persist even among people who regularly process personal information; and the specific legal provisions that allow data to be shared are similarly unclear'

The authors stressed the need for a clearer legislative framework with openness and transparency, the removal of 'unnecessary legal barriers, whilst maintaining robust privacy protections'.[133]

In the House of Lords Report, 'Genomic Medicine', 'the complexities surrounding confidentiality and consent in the sharing of medical data for research purposes' in the UK were referred to as 'burdensome'.[134]

Further and in our more specific context of using PII for medical research, Walport and Thomas suggested that the use of safe havens should be considered as they represent "environments for population based research and statistical analysis in which the risk of

[131] The closest case having been the Collie Case (Common Services Agency v Scottish Information Commissioner [2008] 1 WLR 1550)
[132] Thomas, R and Walport, M (2008) Data Sharing Review Report accessible at http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf
[133] Richard Thomas (the former UK Information Commissioner) has been replaced with a new Commissioner (Christopher Graham) who has a particular vision for data protection regulation with a focus on enforcement and compliance. Sir Mark Walport is Director of the Wellcome Trust, responsible for finding many medical research projects in the UK and abroad.
[134] House of Lords, Science and Technology Committee 2nd Report of Session 2008–09'Genomic Medicine'.

identifying individuals is minimised"[135]. In the context of healthcare in Scotland, different methods for using safe havens to allow linkage between data sets could be considered by data controllers, including ISD.

Very recently, the British Medical Association (BMA), another key informal actor within the governance landscape, has offered principles on releasing patient data for secondary uses, which parallel the current legislative framework. The BMA advises (Local Medical Committees) and practices that where possible, anonymised data should be used in preference to patient identifiable information. Where PII is used, consent should be obtained and where consent has not been obtained, the data can only be used : 1) When s251 NHA Act 2006 is engaged and the common law duty of confidentiality has been set aside as per the ECC; 2) 'the legal and professional criteria for disclosure without consent in the public interest have been met'; and 3 . 'it is a disclosure to a PCT under the 'Confidentiality and Disclosure of Information Directions 2005', which provide a limited statutory basis for some specific disclosures where it is not possible to obtain express consent and where it is not feasible to anonymise data.'[136]

At the time of writing the government is considering a plan to introduce a single Health Research Regulatory Agency (HRRA) which, amongst other goals, would strive to 'simplify' regulation on health research. The HM Treasury 'Plan for Growth' acknowledged the presence of barriers to health research as a key challenge for economic growth within the UK. Healthcare is one area where the plan is striving to 'reduce the stock of regulation', it was noted that within healthcare research, ' National complexity was then compounded by diverse local approval systems, inconsistent, sometimes risk-averse, local interpretations'. The HRRA would be charged with 'streamlining' health research approvals on a national level. The Plan for Growth specifically refers to the great potential of the UK as a world leader in linking large datasets for health research. [137] By the end of 2011, the Department of Health (DoH) will publish a plan and timetable dedicated to giving patients greater control of their records and by Sept 2012, it plans to release the initial data pertaining to the proportion of patients who have greater control of their own records.

[135] Ibid
[136] See BMA (2011) Guidance 'Releasing data for secondary uses'
[137] HM Treasury, Department for Business, Innovation and Skills, 'The Plan for Growth' (March 2011) see http://cdn.hm-treasury.gov.uk/2011budget_growth.pdf (page 8)

In summary, key messages from this chapter are -

- An array of legislative provisions and key formal and informal actors are involved in the current framework governing the use of PII in medical research. The relationships between these provisions and the roles of key actors can contribute to a confusing and complex landscape.
- Such a complex landscape can results in a lack of understanding of data handling obligations for individuals involved in the use of PII.
- The EU Data Protection Directive governs the use of PII within the EEA
- Human Rights considerations should be respected and balanced throughout.
- The Data Protection Act 1998 whilst offering guidance on 'data processing'; however this, in itself, is a vague concept.
- The relationship between the DPA and FOIA is complex, and needs to be clarified however Collie tells us that Data Protection trumps FOI. The challenge is the definition of personal data, something that necessarily involves the EU directive.
- PAC lacks a statutory basis and awarding the authorising body with statutory powers or introducing a statutorily based body with similar functions could be considered.

Having outlined the current framework governing the use of PII in this Chapter, it would be helpful to assess the framework in light of the template discussed in Chapter 3. Chapter 5 is dedicated to this exercise.

Chapter 5 An assessment of how the use of PII is currently governed and associated problems.

Key Questions addressed by this chapter:

- What is the current procedure employed for using PII in medical research?
- What penalties exist for breaching current practice rules?
- What issues relate to the current procedure from the perspective of researchers, data subjects, data processors, regulators and funders?
- Ultimately, how well does the current procedure respond to the necessary components of optimal governance established in Chapter 3?

Key Messages from this chapter:

- It is arguable that an appropriate balance between consent, anonymisation and authorisation is not currently being struck in the Scottish IG landscape.
- While use of PII is authorised by the ECC in England, this has no authority in Scotland where a range of bodies are involved in authorising/advising on data use and sharing. These include PAC, which can be seen to play the key authorisation role, and other entities such as CHIAG and territorial NHS Boards who authorise local or regional uses.
- The role of authorising bodies such as PAC which lacks a statutory basis for its existence may need to be reconsidered and the introduction of a similar body with a statutory basis and a wider remit may need to be considered.
- Data linkages performed between ISD and external data sets should be more widely considered (especially regarding responsibility should DP obligations be breached).[138]

5.1 Current procedure for using patient data – consent or anonymise, with authorisation

[138] Though it should be noted that PAC already considers certain health and non-health linkages for example, linkages between health and police data.

The current practice for using PII in medical research has been identified as being primarily based upon a 'consent or anonymise' approach[139]; where patient consent should be obtained for the use of PII, and where obtaining consent is not possible or practicable, the alternative is to anonymise the data in order to render the data subjects unidentifiable. However, authorisation also plays a key role in this process, as sometimes neither obtaining consent nor anonymisation of PII are possible, the use of such PII must then be authorised, a role fulfilled in Scotland by PAC with respect to many but by no means all datasets. PAC is restricted to advising ISD and NRS regarding datasets they hold, such as, for example, SMR datasets. Individual health boards do not rely on PAC, but on Caldicott Guardians. Thus a plethora of actors are involved in authorising data use and sharing, while consent and anonymisation systems may be being used inappropriately or sub-optimally depending on circumstances. There is no comprehensive study showing the nature and range of governance mechanisms currently deployed in the country.

5.2 How well does the current procedure respond to governance requirements?

We will now use the key questions established in Chapter 3 to test the current models effectiveness in fulfilling necessary governance requirements.

1) Is the model fit for the purposes that it is designed to achieve, now and in the future?

The public engagement stream of SHIP is currently gathering empirical evidence on this question. From a legal and regulatory perspective, however, the above discussion would suggest that the current model is flawed. Indeed tentative findings from the Public Engagement stream of SHIP echo the criticisms of the current landscape as they appear within the dominant literature. At the time of writing, a joint article between the Information Governance and Public Engagement steams of SHIP is under preparation. Our findings will be published in due course.[140]

[139] AMS Response to Data Sharing Review – see www.acmedsci.ac.uk/download.php?file=/images/publication/...pdf

[140] Findings from the PE/IG Workshop on Researchers and Trust, held at the SHIP Biannual Conference at St Andrews, September 2011

2) How does the model reflect public expectations and impact on public confidence?

ISD attempt to observe the highest of DP standards and good reputation is a priority. The current procedure in place does ensure that staff are informed of their obligations and disciplined where breaches occur. Nonetheless it is inevitable that data mishandling whether ISD related or not, will shake the public confidence in the use of PII for medical research. NHS Boards are required to improve their patient information on the range of healthcare issues of PIU by means of the Information Governance standards, part of the NHS QIS CGRM (National Health Service Quality Improvement Scotland Clinical Governance and Risk Management) standards and ISD and HPS (Health Protection Scotland) do offer a wide array of information to the public via their websites. Notwithstanding this piecemeal approach, there has never been a nationwide education campaign such as that advocated and recommended by CSAGC and evidence to date suggests that there is widespread lack of knowledge and understanding of current data use and sharing practices.

3) How does the model fare when it undergoes a PIA (Privacy Impact Assessment)?

Whilst a PIA has been carried out at ISD, most recently in 2008, changes will have been made based upon recommendations of the assessment, and thus a new PIA would need to take place in order to give an accurate account of potential risks with current procedure. It is not clear that PIAs have been adopted across the range of actors involved in the current IG landscape in Scotland; indeed, the lack of joined-up governance suggests that there are increased risks to privacy within current arrangements.

4) How is the model monitored/regulated?

Refer to Chapter 4 for a detailed outline of the current governance of PII in medical research. Numerous bodies claim an oversight or governance role in the present climate including Scottish Government, the Chief Scientist's Office, NSS, ISD, Health Boards, Caldicott Guardians, Directors of Public Health, GPs and individual health care practitioners.

5) Do all parties involved understand the implications of a particular model?

As previously mentioned, legislation in this area, particularly the vague DPA 1998 and the varying interpretations of the Data Protection Directive in light of the margin of appreciation granted to member states is confusing. Consequently, the question of whether informed consent is required for the secondary use of PII in research is a bone of contention. Lord Falconer has responded stating '"Data can be used for any medical research purpose under the [Data Protection] Act, without the need for the consent of individuals'.[141] However, he then stresses that it is the common law which demands that informed consent from patients be obtained, unless it can be argued that use without consent is in the public interest, which is an uncertain concept in itself. Thus, in summary, unless one is willing to rely on a public interest defence should their use of PII without consent be questioned; the default is to anonymise data.

In terms of ISD procedure, staff members are informed of their data protection obligations during their employee induction, after which they must sign a document which states that they agree to uphold these obligations in adherence with the confidentiality guidance they are given. The guidance covers all aspects of DP issues, including, importantly in this context, types of data which can and cannot be communicated. Subsequently, each ISD employee must sign a similar document each year, to the same effect. Recipients of ISD data must also meet certain criteria in relation to data security etc – these are determined as part of the PAC application process.

Anecdotal evidence suggests that researchers, users and publics alike are unclear about current protections and possibilities within the present system.

6) What vetting and training methods will be implemented in any model?

Here, it is more appropriate to look at what methods are currently implemented at ISD as an example of best practice.

[141] Lord Falconer of Thoroton (2001) BMJ 'Privacy law and medical research' [letter]. *Times* 2001 May 17: 21 http://www.bmj.com/cgi/content/full/328/7447/1029

Applicants are asked to inform ISD about the data security/confidentiality training that the recipient analysts have had, thus ISD do not provide training but rather, make a judgement of suitability based on the analyst's prior experience.

ISD do not carry out vetting either, they simply ask for names, institutions and other relevant details of analysts. However in terms of the data custodian associated with the application, they do check that the name provided is for someone who is professionally registered (usually this involves checking the GMC website). Usually there will be email/phone contact with applicant during the course of their application. Many (but certainly not all) applicants are regulars with whom a relationship has developed.[142]

7) Is there accountability in the model and who is accountable at each stage in any model?

Sanctions imposed by and upon key actors in the current legislative framework have been discussed in Chapter 4. In summary, where DP obligations are not met, researchers risk refusal to PII access and subsequently jeopardising their present and future projects completely. Data processors risk financial penalties, staff members risk disciplinary action and potentially, dismissal. The most serious offences can be penalised with a custodial sentence for a maximum of 2 years.

As indicated earlier, since receiving his new powers the ICO has issued fines and has not discriminated between public and private bodies, the lack of adequate security measures, and in particular, encryption methods has provided grounds for penalty on more than one occasion[143], highlighting the need to implement appropriate security measures for data transfer between organisations.

At ISD, where non-observance of data protection obligations is noted, employees may be disciplined or dismissed, depending on the gravity of the inappropriate use of PII. Dismissal however, is carried out only exceptionally and any errors are usually discussed and dealt with internally.

[142] The PAC application form offers an idea of what ISD look for - http://www.isdscotland.org/isd/3051.html
[143] For a list of ICO 'undertakings, enforcement and monetary penalties' see http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx#undertakings

However, it is suggested that ISD relies more on a strong desire to uphold a good reputation, both from their own part, and the part of those requesting data than a hard-lined approach to ensuring compliance. After all, the wealth of data available is so valuable to researchers, and Scotland is relatively small in that where a reputation for good DP standards is tarnished, this itself may impede access to data substantially. It should also be noted that part of ISDs statutory purpose is 'to collect and disseminate epidemiological data and participate in epidemiological investigations'.

Once again, anecdotal evidence suggests that many actors, including data controllers, are unclear about their roles and responsibilities.

8) Who are the stakeholders and are they satisfied?

An important aim of this paper is to highlight any problems or gaps in the existing legislative framework and procedures used, in terms of facilitating research and minimising risk, concerns relating to key parties affected by and involved in the research procedure should be considered.

Researchers

Researchers, the actors actually carrying out the medical research are faced with hurdles from the beginning of their projects. Whilst PAC attempts to lay out in as clear terms as possible the privacy requirements which must be met for a successful application to access PII, DP obligations under the law can be confusing. Projects can be abandoned as a result of failure to obtain PAC authorisation due to lack of understanding of DP requirements as opposed to a lack of willingness to adhere to them and ultimately, this can result in lost funding. The relationship between PAC and REC bodies is unclear.

Data Subjects

Although this is a problem almost impossible to resolve without greatly impeding medical research using PII, we cannot ignore the argument that data subjects cannot offer fully informed consent to what use their PII is put because researchers cannot envisage every potential future data linkage for one particular set. This is particularly relevant for linkages between health and non-health datasets which may potentially be

the most privacy invasive types of linkages. As mentioned earlier, an MRC survey is one amongst several studies which highlight the public's lack of understanding of the use of PII in medical research. Conflicting evidence regarding public attitudes in this area exists. Clear understanding of what the public expect and need is lacking, Scottish-based evidence is particularly scarce. It is hoped that the Public Engagement stream of SHIP will gather valuable insight in this area.

Data Controllers and Data Processors

Where the law is confusing for researchers, it can be even more so for data controllers and data processors like ISD who must at all times keep in mind DP obligations whilst performing an array of tasks. ISD must ensure PII received has been obtained lawfully, that it is processed lawfully and that where requests for data sharing are made, the organisation making the request has legally acceptable standard of DP procedures in place itself. Further, as mentioned previously, the distinction in roles and responsibilities between data controllers and processors is often unclear, particularly given the potential overlap of roles within smaller organisations. The Article 29 Data Protection Working Party has offered guidance on the respective roles and responsibilities of these actors, in particular it stresses that there should be a clear line of accountability throughout the data transfer process.[144]

Thomas and Walport point out that for individuals such as GPs, who may be frequently faced with data sharing requests and lacking in clear procedures, *'the absence of clear legal advice typically results in one of two outcomes. People either make decisions based on what feels right to them as professionals, albeit with concerns that their approach may not accord exactly with the law. Or (and perhaps the greater temptation for many) they defer decisions altogether, for fear of making a mistake'.*[145]

Funding bodies

Whilst proposals submitted for funding may appear attractive investments to funders, failure of researchers to gain PAC or REC authorisation or upholding DP requirements may cost mean supplying additional funding.

[144] Article 29 Data Protection Working Party (2010) Opinion 1/2010 on the concepts of "controller" and "processor" see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf
[145] Thomas and Walport 'Data Sharing Review Report' (2008)

Regulators/Authorising Bodies

First, we consider the role of authorising/advisory bodies, namely in Scotland i.e. the role of the Privacy Advisory Committee for Scotland (PAC).

The question has arisen at various juncture as to whether PAC or a similar-type body should enjoy statutory existence and a remit that extends on a more national level. The obvious precedent is the experience south of the border with the EEC. This could be an opportunity to streamline approval procedures, although it would require buy-in from data controllers around the country, and most notably Caldicott Guardians in each of the health Boards. Matters are complicated further if sharing with entities outside the NHS is contemplated.

We should consider governance issues which may come up where data requests are made both for and from PII data held in non-EEA countries, where the European Data Protection Directive does not apply, and data protection standards may differ. Here the importance of mutual recognition of equivalent standards arises.

Even within EEA member-states, it can be argued that 'harmonization remains more apparent than real'[146], thus privacy requirements, such as patient consent, may be subject to conflicting conditions between different national frameworks as well as between different legal and ethical frameworks of a single Member State.'[147]

9) How does the model sit within the legal order?

The anonymisation of data is seen as a way of bypassing consent obligations because the patients are no longer identifiable as a result of the stripping off of any identifiers before use for research. However, it can be argued that anonymisation is never 100% possible, thus the patients could be identified, whilst highly unlikely, the possibility exists. If PII has been used without an individual's consent, then the individual who has disclosed this data may be liable for breach of confidentiality. Thus, the lawfulness of the consent or anonymise approach, that most often employed, can be brought in to question.

[146] Rahmouni et al (2009) 'Modelling and Enforcing Privacy for Medical Data Disclosure across Europe' in Medical Informatics in a United and Healthy Europe' K P Adlassnig et al, IOS Press, 2009

[147] ibid at 695

The lack of enforcement powers belonging to the Information Commissioner's Office have been mentioned previously, in order to ensure data protection compliance to a high standard, higher deterrence factors such as increased penalties for data breaches should be considered.

The lack of an obvious legal basis for authorising/advisory bodies is a continual concern.

10) Does the model add value to and improve upon the inadequacies of existing mechanisms?

This question relates to potential models which will be considered by ISD and SHIP in due course.

11) Does the model reflect a proportionate approach to governance?

As outlined above, a recurring complaint against the current landscape is that it is over-burdensome and that governance mechanisms are at times disproportionate. Indeed, this was one of the drivers for the AMS Report which emphasised the need for proportionate governance. The lack of certainty which researchers often encounter due to the complex and varying legislative provisions, and the numerous approvals which researchers must navigate through before accessing (often low risk) datasets all suggest that in terms of proportionality, the current landscape leaves room for improvement.

5.3 Uses of the data – research, linkage with other data sets outside NHS/ISD. Who is responsible for the data?

Next, is the issue of the linkage of data sets between NHS/ISD and other external data sets. Researchers may wish to link health data with, for example, educational data, or police records. Where ISD must determine whether or not to perform requested linkages and share this data with the requestor, usual practice dictates obtaining prior approval from PAC and ensuring that the recipient holds satisfactory security standards and that the processing purpose is compatible with that of ISD.

Once the data are with the external recipient, ISD views them not as a data processor in DPA terms but more so as a data controller (DC), thus, all responsibilities for the data

processing, in ISDs view, lies with the new data controller. However, it may be argued that the responsibility could be joint. It is argued that this needs to be more surely established. The current view is that ISD are disclosing data in accordance with their statutory role and register entry with the Information Commissioner. However we should consider the SWISS Database[148] which keeps track of employees in NHS Scotland, where 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. So, it is possible to agree about stakeholders who will be a data controller (and a fortiori data processor) and on what basis

A joint DC role would involve substantially more work, likely onerous given the potential number of key actors, to establish properly. Whilst, in the instance of a data breach involving the ISD supplied data, it is the DC who will carry out incident management, ISD demands that data recipients report any inappropriate use of the data to a Caldicott Guardian or directly to ISD where an incident report is made. Subsequently, ISD may review their willingness to share data with the DC in the future; the decision will be largely based on how the DC responded to the incident.

In summary, key messages from this chapter are -

- Key stakeholders in the project and its success can be identified as - researchers, data subjects, data processors, regulators/authorising bodies and funding bodies.
- Given the confusing nature of the law, it is doubtful that at present, all parties fully understand the legal requirements to which they are subject.
- Whilst some accountability exists under the current procedure, greater deterrents or incentives could be used in order to promote a more DP sensitive culture.
- Data controllers, in particular GPs, may shy away from responding to data sharing requests due to uncertainty of the law and fear of sanctions.

[148] NHS Scotland SWISS (Scottish Workforce Information Standard System) see http://www.isdscotland.org/isd/6127.html#SWISS

- The powers of regulators are at present limited, in particular, the role of PAC and its lack of statutory powers should be reconsidered
- Governance issues for data requests between EEA and non-EEA countries should be considered
- It is important to consider linkages of health and non-health data sets
- Proportionate governance is vital in removing unnecessary hurdles to data linkage whilst simultaneously ensuring adequate protection mechanisms where they are needed

Part 3 – Forecast for the future

Chapter 6 Forecasts for the future

Key Questions addressed by this chapter are -

- What are the key arguments for and against attributing PAC or a PAC-like body with statutory powers?
- What are the pros and cons of linking health and non-health data sets?

Key Messages from this chapter are -

- Awarding PAC or a PAC-like body with statutory authority may serve to legitimate the authoritative role it currently plays; a wider remit can also be contemplated.
- The potential advantages from performing health and non-health data linkages must be balanced carefully.

6.1 Potential changes in legislation, recent increased powers for ICO and PAC

The future framework…new actors, legislation and guidance

Key Messages

- The Scottish Government Draft Principles may affect the way that PII data are shared beyond the health setting
- To date, the ICO has relied heavily on voluntary compliance.
- The recent increase in ICO powers in the form of monetary fines may render a previously 'toothless' actor more powerful

Having explored the pre-existing governance framework in this area, it is worthwhile noting that the framework is constantly evolving, with new actors, legislative provisions, guidelines and advisory bodies entering and old ones leaving. This section looks towards the future changes which may result, and the effects they might have on the dynamics of the current framework.

Scottish Government Draft Identity Management and Privacy Principles (the Draft Principles)

The Draft Principles are designed to promote good practice amongst public service organisations. At the moment of writing, we await the results of the consultation on the Draft Principles. In short, the proposed principles echo pre-existing regulations and guidelines on data protection and privacy.[149] Of note, in relation to data and data sharing, the draft principles recommend that *'If a public service organisation needs to link personal information from different systems and databases, it should avoid sharing persistent identifiers; other mechanisms, such as matching, should be considered. If a public service organisation believes that persistent identifiers should be shared, it must publicly explain why.'*[150]This raises questions about sharing or linkage of PII with agencies beyond the health sector.

Increase in ICO powers

The ICO itself has acknowledged its lack of enforcement powers, commonly referred to as its 'lack of teeth'[151]. It relied heavily on voluntary compliance of those handling PII. Further, Kaye and Gibbons note that 'it appears to deploy its investigative and enforcement powers only in extreme circumstances, where public scandals erupt, or in response to formal complaints by data subjects'[152].

However, after substantial lobbying, and as we have seen, the ICO now has the power to impose fines of up to £500,000 for serious DPA breaches.[153]The extent to which the ICO exercises his discretion in determining whether or not to penalise an organisation and to what extent this raises awareness of and deters future breaches remains to be seen but early indications suggest that the powers will not lie dormant. It will be important that all individuals involved in using PII are made aware of these new fines, to assist in generating a culture of best practice in data handling.

[149] Scottish Government 'Privacy and Public Confidence in Scottish Public Services: draft Identity Management and Privacy Principles' accessible at http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation/Q/Page/8
[150] Ibid
[151] Holyrood DP Conference (2009)
[152] Kaye and Gibbons (2008) at 120 see n2
[153] ICO, new penalties, see http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties_guidance_120110.pdf

Having discussed both recent changes and potential future changes in the landscape, it is worthwhile here to consider the potential pros and cons of increases in authorising body powers, specifically relating to PAC.

Allocating PAC or a PAC-like body with statutory powers

Pros

- Although it is an advisory committee to an NHS Board which is acting intra vires, PAC's legitimacy given its lack of statutory basis, has been questioned. Perhaps the introduction of a statutory basis for PAC, or introducing a similar body might help to clarify and consolidate its role.
- Endowing PAC with statutory powers could invite more proposal applications and more adherence to PAC codes.
- A PAC-like body with a statutory basis and a wider remit could be the basis for a more efficient operationalisation of governance mechanisms within Scotland

Cons

- Although lacking in statutory basis, PAC already exerts considerable influence, arguable almost equal influence to statutorily based RECs in England, it is questionable whether an increase in powers would change the current status quo regarding compliance.
- The law may ossify the body and not allow sufficient flexibility to respond to future development.
- Any increased authority and stature would subsequently increase PAC's workload and this would have to be resourced as at present, the Committee relies on members' voluntary contributions to the workload.
- A PAC-like body with a wider remit might not find support across the range of stakeholders that would require to buy-in to its role.

6.2 Hierarchies of data linkage – intra NHS/ISD linkage as well as external public-private linkage implications i.e. the ethical pros and cons of combining health and non-health data sets

Whichever model SHIP/NHS/ISD adopts, it will need to be one which facilitates linkage of data sets not only within the health service but with external data sets, both of a public and private nature. The implications of such linkages should be considered, of particular concern here are the ethical implications of combining health and non-health data sets.

Performing non-health data linkages with health-related data sets is common for many research studies, particularly those related to social welfare[154] throughout the world. Australia has been acknowledged as one of the leading countries in the context of health research using data linkage. The WADLS (Western Australian Data Linkage System), which has been running since 1995, has been responsible for linkages to both local and national health welfare datasets.[155]Amongst other benefits of such linkages, it is claimed that ' *data linkage has conserved patient privacy; community machinery necessary for organised responses to health and social problems has been exercised; and the commercial return on research infrastructure investment has exceeded 1000%. Most importantly, there have been unbiased contributions to medical knowledge and identifiable advances in population health arising from the research.'*[156]

The pros and cons of combining health data with external data sets.

Potential benefits of such linkages

- Such linkages can often be more 'cost efficient' in comparison with 'more traditional approaches to epidemiologic and health services research'
- 'Adding value to existing information assets and generating a research return on the substantial existing investment in routine administrative and clinical data sets within health.'[157]

[154] For example, the Nuffield Trust has carried out work on linking health and social care data for predictive risk analyses. See Lewis et al, 'Developing a model to predict the use of social care' (2008) in Journal of Care Services Management. Accessible at http://www.nuffieldtrust.org.uk/media/detail.aspx?id=48&prID=563

[155] Holman CD et al (2008) 'A decade of data linkage in Western Australia: strategic design, applications and benefits of the WA data linkage system', PMID: 18980573 see http://www.ncbi.nlm.nih.gov/pubmed/18980573

[156] ibid

[157] Australian Government National Collaborative Research Infrastructure Strategy 'Population Health and Clinical Data linkage' http://ncris.innovation.gov.au/Documents/PopHealth_Roadmap.pdf

- Health and non-health data linkages can facilitate 'integration of data from the health sector with a wide range of data from other sectors (including, for example, education, community services, police, justice, planning, transport), without the requirement for unique personal identifiers across these sectors.'[158]
- Thus, research which combines ISD data sets with data from various non-health sectors has the potential to provide insight into these areas as well as driving necessary improvements.

Potential problems with external data linkages

- 'Concerns involving confidentiality caused by geographically referenced health information'[159]
- Respect for patient privacy and maintaining confidentiality are important concerns. Where data is linked with external organisations, confidentiality may be at risk, it is important that these organisations have guidelines for DP obligations in similar terms to those at ISD.[160]
- It can be argued that public-private data linkages may give rise to profiteering from private organisations.
- The challenges of ensuring adequate, effective and joined-up governance across sectors.

In summary, key messages from this chapter are -

- The recent increase in ICO powers, if they are to be used in practice and not just present in theory, may promote higher standards of DP practice
- Allocating statutory authority to PAC or a PAC-like body could serve to legitimate the functioning as a Scottish authorising body

[158] ibid

[159] Olvingson C et al (2002) ' Ethical issues in public health informatics: implications for system design when sharing geographic information' in Journal of Biomedical Informatics Volume 35, Issue 3, June Pages 178-185

[160] It should be noted that relevance and importance of different concerns will vary depending on which stakeholder is consulted, what may be a primary concern to a researcher may be different to that of a member of the public.

- Whichever model is chosen, it must continue to facilitate data linkage between health and non-health data and promote more potentially valuable linkages of this kind
- Care should be taken not only to maximise potential research benefits in health/non-health linkages, but also to minimize potential risks.

Part 4 - Recommendations

Chapter 7: Recommendations from report and summary of key messages

7.1 General Considerations

- Respect for patient privacy and the public interest are both core guiding principles, whilst they are often competing considerations, a balance between the two should be sought. In fact, the UK Information Commissioner suggests that maintaining patient privacy can be in the public interest at times.[161]

- Choice, anonymisation and authorisation-based approaches are available models, however whilst reconciling competing interests in each model can be difficult, these approaches are not mutually exclusive.

- Anonymisation of PII is an option, however it is not without its limitations; no data can be fully anonymised and PII is still being used without consent.

7.2 Current Legal Landscape

- Whilst the legal landscape governing PII differs between England and Scotland, governance is sub-optimal in both areas and changes are recommended to improve the situation in Scotland.

- The current framework consists of unclear legislation and professional guidelines. Legal and professional obligations of all actors involved in the use of PII should be clearly understood. Clarification of the law and better training of all involved in dealing with PII may offer some solutions.

- The creation of an appropriate authorising body with similar functions to PAC, but with a wider remit, and perhaps with a statutory basis to clarify and legitimise its function, should be considered

[161] ICO, 'FOIA: The duty of confidence and the public interest' (2008), accessed at - http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/sec41_confidence_public_interest_test_v1.pdf

7.3 Optimal Governance

- Optimal governance should embody a coherent and transparent framework, with clear and simple principles and procedures for researchers to follow.

- Proportionate approaches to governance are essential. The level of scrutiny against which applications to access data are held should accurately reflect the perceived level of potential risk such data linkages might have.

- Choice, anonymisation and authorisation based approaches can be considered alone or in combination.

- Terminology in this area should be unified.

- In testing any potential governance model, a template consisting of 10 key questions can be used -

1) Is the model fit for the purposes that it is designed to achieve, now and in the future?

2) How does the model reflect public expectations and impact on public confidence?

3) How does the model fare when subject to a PIA (Privacy Impact Assessment)?

4) How is the model monitored/regulated?

5) Do all parties involved understand the implications of the particular model?

6) What vetting and training methods will be implemented in any model?

7) Is there accountability in the model and who is accountable at each stage in any model?

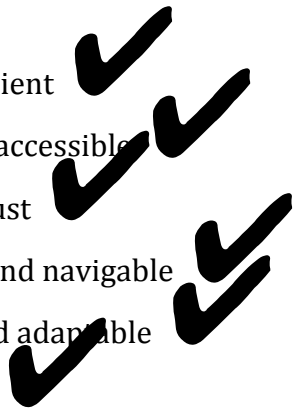
8) Who are the stakeholders and are they satisfied?

9) How does the model sit within the legal order?

10) Does the model add value to and improve upon the inadequacies of existing mechanisms?

11) Does the model reflect a proportionate approach to governance?

Overarchingly, a system should be:



- Effective and efficient
- Transparent and accessible
- Procedurally robust
- Understandable and navigable
- Proportionate and adaptable
- Legal and ethical

- Privacy Impact Assessments may be a useful tool in monitoring potential privacy risks prior to the implementation of any particular model; they should be employed in the project.

- The implications of external and internal linkage of data sets should be considered, particularly with regards to legal obligations where sharing data between EEA and non-EEA States.

- An optimal model would include penalties which whilst not excessive, have enough power to deter researchers from breaching their obligations when handling PII.

7.4 Public Engagement

- Not enough is currently known about public attitudes to use of PII in medical research. Due to the lack of information on public attitude and trust, bodies such as PAC must make their own assumptions of what uses of PII the public would or would not accept. More information on public attitudes must be gathered, in particular, on what expressions of control are available, and how to engender trust of and amongst researchers.

- Information campaigns should be employed to better inform the public of the potential benefits of research and to raise public confidence. Perhaps we should also stress the importance of including information on the potential risks involved with research, allowing the public to make better informed choices.

- In order to promote public confidence, high standards of research practice should be met during all aspects of the research process, from procuring PII, to using it, to storing it.

Acknowledgements

We should like to thank all those who gave up their time to participate, particularly those involved with the Scottish Health Informatics Programme, too numerous to mention as part of such a diverse collaborative team. We trust that you know who you are. We are, none the less, particularly grateful to Patricia Ruddy at NHS Information Statistics Division for her particularly strong contribution to the paper. All errors are the responsibility of the authors.

References

Academy of Medical Sciences (2006) 'Personal Data for public good: using health information in medical research' www.acmedsci.ac.uk/download.php?file=/images/project/Personal.pdf

Academy of Medical Sciences (2011) ' 'Personal data for public good: using health information in medical research' see http://www.acmedsci.ac.uk/p118pressid46.html

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

Al-Shahi R, Vousden C and Warlow C 'Bias from requiring explicit consent from all participants in observational research: prospective, population based study' *BMJ 2005;331:942*

Article 29 Data Protection Working Party (2010) Opinion 1/2010 on the concepts of "controller" and "processor" see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Australian Government National Collaborative Research Infrastructure Strategy 'Population Health and Clinical Data linkage' http://ncris.innovation.gov.au/Documents/PopHealth_Roadmap.pdf

Barrett G et al (2006) 'National survey of British public's views on use of identifiable medical data by the

National Cancer Registry' BMJ 332:1068-1072

Brazier M, Cave E (2007) 'Medicine, patients and the law' 4th Edition London: Penguin,

British Medical Assosciation (2011) Guidance on 'Requests for disclosure of data for secondary purposes' see http://www.bma.org.uk/images/releasingdataforsecondaryuses_tcm41-208763.pdf

Cabinet Office, 'Cabinet Secretary publishes plan to improve data security' http://www.cabinetoffice.gov.uk/newsroom/news_releases/2008/080625_data_security.aspx

Caldicott Guardian Circular for CGs in England http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4011935.pdf

Clark A, ESRC NCRM (Economic and Social Research Council National Centre for Research Methods) Working Paper (2006) 'Anonymising Research Data'

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

Common Services Agency v Scottish Information Commissioner [2008] 1 WLR 1550 - http://www.itspublicknowledge.info/applicationsanddecisions/Decisions/2005/200500298.asp

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

Department of Health (2009) Consultation Report : 'Consultation on the additional uses of patient data' accessible at http://www.dh.gov.uk/en/Consultations/Responsestoconsultations/DH_109310

Department of Health, the Caldicott Committee, 'Report on the Review of Patient-Identifiable Information' 1997

Department of Health, 'NHS Caldicott Guardians' http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563

Data Protection Act (1998)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data

ESRC Working Paper 'Anonymising Research Data', (2006) ESRC National Centre for Research Methods

European Commission, Article 29 Data Protection Working Party website at - http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

European Data Protection Supervisor, 'The European Guardian of Personal Data Protection' http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

Fairhurst J and Vincenzi C (2003), 'Law of the European Community' (4th Ed.), Pearson/Longman, London

Freedom of Information Act 2000 (FOIA)

Freedom of Information (Scotland) Act 2002

'Freedom of Information (Scotland) Act 2002 - A guide for the Information Professional' at http://www.slainte.org.uk/files/pdf/foi/foisa04.pdf

GMC (General Medical Council) Confidentiality Guidance (2009) - http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_contents.asp

GMC, 'About us - Legislation' http://www.gmc-uk.org/about/legislation.asp

Handyside v United Kingdom *(*1976*) 1 EHRR 737*

Health Protection Scotland accessible at http://www.hps.scot.nhs.uk/

Health Insurance Portability and Accountability Act (HIPAA) 1996 (USA) http://www.hipaaguide.net/

Health and Social Care Act 2001

Hi-Tech Scotland (2009) 'Scottish public lose faith in UK Government's data-handling' accessed at http://www.hi-techscotland.com/article/09-02-09__scottish-public-lose-faith-in-uk-governments-datahandling

HM Treasury, Department for Business, Innovation and Skills, 'The Plan for Growth' (March 2011) see http://cdn.hm-treasury.gov.uk/2011budget_growth.pdf

Holman CD et al (2008) 'A decade of data linkage in Western Australia: strategic design, applications and benefits of the WA data linkage system', PMID: 18980573 http://www.ncbi.nlm.nih.gov/pubmed/18980573

Homer et al (2008) 'Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping micro arrays' in Public Library of Science Genetics J 4:e1000167

House of Lords, Science and Technology Committee 2nd Report of Session 2008–09 'Genomic Medicine' accessible at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf

Human Rights Act 1998 Article 8 Right to respect for private and family life accessible at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_3

Information Commissioner's Office - http://www.ico.gov.uk/about_us.aspx

Information Commissioner's Office (2010) Penalties Guidance , see http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties_guidance_120110.pdf

Information Commissioner's Office (2009), 'Privacy Impact Assessment', Handbook - accessible at http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

Information Commissioner's Office (2002) Chapter 4, 'Use and Disclosure of Health Data, Guidance on the application of the Data Protection Act 1998' accessible at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf

Information Commissioner's Office, 'The Freedom of Information Act: Your rights, responsibilities and obligations to freedom of information' http://www.ico.gov.uk/what_we_cover/freedom_of_information.aspx

Information Commissioner's Office Press Release (2008) 'ICO welcomes new powers to fine organisations for data breaches' see - http://www.ico.gov.uk/upload/documents/pressreleases/2008/criminal_justice_and_immigration_act.pdf

Ipsos MORI (2007) 'Keeping It Confidential: Public Attitudes Towards The Use Of Personal Health Information In Medical Research', accessed at http://www.marketresearchworld.net/index.php?option=com_content&task=view&id=1498&Itemid=77

JISC, 'Freedom of Information Act 2002: Implementation and Practice (Scotland) at http://www.jisc.ac.uk/publications/d

ocuments/pub_ib_fois.aspx#05enforcement

Joseph Miller & Co Chartered Accountants, 'First Data Protection Act fines issued' (2001) see http://www.joseph-miller.co.uk/ard/enews_article.asp?ID=2278&AID=816&CID=1

Kaye J and Gibbons S, 'Mapping the regulatory space for genetic databases and biobanks in England and Wales', Medical Law International, 2008, Vol 9, pp111-130

Laurie G, Genetic Privacy: A Challenge to Medico-legal Norms (2002, Cambridge University Press).

Laurie, G, "Reflexive Governance in Biobanking: On the Value of Policy Led Approaches and the Need to Recognise the Limits of Law' (2011) 130(3) Human Genetics 347-56.

Laurie G and Gertz R (2009) 'The Worst of All Worlds? Common Services Agency v Scottish Information Commissioner', EdinLR Vol 13 pp 330-334

Lord Falconer of Thoroton (2001) BMJ 'Privacy law and medical research' [letter]. *Times* 2001 May 17: 21 http://www.bmj.com/cgi/content/full/328/7447/1029

Lowrance W (2003) 'Learning from experience: privacy and the secondary use of data in health research' in J Health Serv Res Policy Vol 8 Suppl 1 July 2003 S1:5

Mason JK, Laurie GT, (2010) 'Law and Medical Ethics, 8th Edition', Oxford University Press

Medical Research Council, Data and Tissues Tool Kit, 'Seeking Approvals: Privacy Advisory Committees' http://www.dt-toolkit.ac.uk/routemaps/station.cfm?current_station_id=430

National Health Service Act 2006 accessible at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060041_en_1

NHS Connecting for Health. Data Safe Havens accessible at www.connectingforhealth.nhs.uk/systemsandservices/.../safehaven

NHS Connecting for Health, 'Caldicott Guardians' - http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

NHS 'Caldicott: Principles into Practice'

http://www.wales.nhs.uk/sites3/page.cfm?orgId=783&pid=31174

NHS National Research Ethics Service, 'The role of RECs', at http://www.nres.npsa.nhs.uk/aboutus/about-recs/role-of-recs/

NHS National Services Scotland (2005) 'NHS Information Governance Standards' accessible at - http://www.shb.scot.nhs.uk/initiatives/informationgovernance/documents/IG_Standards_FINAL_22122005.pdf

NHS HDL (2003) 37 'The use of personal health information in NHS Scotland to support patient care' http://www.show.scot.nhs.uk/sehd/mels/HDL2003_37.pdf

NHS MEL 19 (1999) Caldicott Guardians in Scotland, see http://www.show.scot.nhs.uk/Publications/index.asp?offset=2884

NHS NSS, ISD Scotland, 'Our Organisation' accessed at http://www.isdscotland.org/isd/3352.html

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

NHS Scotland SWISS (Scottish Workforce Information Standard System) see http://www.isdscotland.org/isd/6127.html#SWISS

NIGB, 'Database Monitoring Sub-group' see http://www.nigb.nhs.uk/ecc/dmsg

Nuffield Trust, Lewis et al, 'Developing a model to predict the use of social care' (2008) in Journal of Care Services Management

http://www.nuffieldtrust.org.uk/media/detail.aspx?id=48&prID=563

Olvingson C et al (2002) ' Ethical issues in public health informatics: implications for system design when sharing geographic information' in Journal of Biomedical Informatics Volume 35, Issue 3, June Pages 178-185

PN Furness and M L Nicholson (2004) 'Obtaining Explicit Consent for the Use of Archival Tissue Samples: Practical Issues' 20 J Med Ethics 561

Rahmouni et al (2009) 'Modelling and Enforcing Privacy for Medical Data Disclosure across Europe' in Medical Informatics in a United and Healthy

Europe' K P Adlassnig et al, IOS Press, 2009

Regidor E, 'The use of personal data from medical records and biological materials: ethical perspectives and the basis for legal restrictions in health research' (2004) in Social Science and Medicine (54) 1975-1894

R v Secretary of State for *Health*, *ex parte Source Informatics*, [2002] QB 424 CA

Scottish Executive Health Department (2006) 'Research Governance Framework for Health and Community Care', see http://www.cso.scot.nhs.uk/publications/ResGov/Framework/RGFEdTwo.pdf

Scottish Executive Health Department, NHS HDL (2003) 37, ' The use of personal health information in NHSScotland to support patient care.' See http://www.sehd.scot.nhs.uk/mels/hdl2003_37.pdf

Scottish Government, Privacy Principles Consultation 2009 accessed at http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation/Q/Page/8

Scottish Government 'Privacy and Public Confidence in Scottish Public Services: draft Identity Management and Privacy Principles' http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation/Q/Page/8

Scottish Government 'Freedom of Information - the Scottish Government's Six Principles' http://www.scotland.gov.uk/About/FOI/6principles/Q/EditMode/on/ForceUpdate/on

Scottish Government Emergency Care Summary - http://www.scotland.gov.uk/Publications/2006/08/16152132/0

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

Thomas, R and Walport, M (2008) Data Sharing Review Report accessible at http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf

Walley T (2006) 'Using personal health information in medical research: Overzealous interpretation of UK laws is stifling epidemiological research' in BMJ. 2006 January 21; 332(7534): 130–131

Wellcome Trust (2009) Report - 'Towards Consensus for best practice - use of patient records from general practice for research' accessible at http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtx055660.pdf

Wellcome Trust Policies and Positions for use of personal information in research http://www.wellcome.ac.uk/About-us/Policy/Spotlight-issues/Personal-information/Policiesandpositions/index.htm

APPENDIX

TABLE OF ABBREVIATIONS

ABBREVIATION	EXPANSION
BMA	British Medical Association
CG	Caldicott Guardian
CHI	Community Health Index
CHIAG	Community Health Index Advisory Group
CMO	Chief Medical Officer
CSA	Common Services Agency
CSAGS	Confidentiality and Security Advisory Group for Scotland
DC	Data Controller
DP	Data Protection
DPA	Data Protection Act 1998
ECC	Ethics and Confidentiality Committee
ECHR	European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms)
EDPS	European Data Protection Supervisor
EEA	European Economic Area
FOIA	Freedom of Information Act 2000
FOISA	The Freedom of Information (Scotland) Act 2002
FPN	Fair Processing Notice
GMC	General Medical Council
GP	General Practitioner
HRRA	Health Research Regulatory Agency
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
LMC	Local Medical Committee
MILA	Multi Institutional Linkage and Anonymisation
MRC	Medical Research Council
MREC	Multi-centre Research Ethics Committee

NHS NSS ISD (ISD)	National Health Service National Services Scotland Information Statistics Division
NIGB	National Information Governance Board
NSS	National Services Scotland (part of NHS)
NRS	National Records of Scotland
PAC	Privacy Advisory Committee for Scotland
PIA	Privacy Impact Assessment
PIAG	Patient Information Advisory Group
PII	Person Identifiable Information
PN	Privacy Notice
REC	Research Ethics Committee
SG	Scottish Government
SHIP	Scottish Health Informatics Programme
SHIS-R	Scottish Health Information Service for Research
SIC	Scottish Information Commissioner
SMR	Scottish Morbidity Record