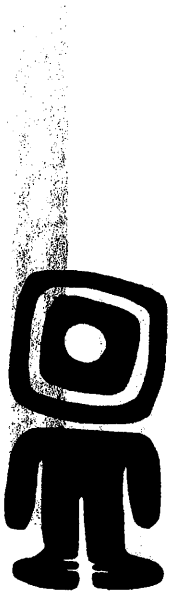

Humanitas Research

Does Northern Ireland need an equivalent to Section 60 of the Health and Social Act 2001?

A Report to the Privacy Advisory Committee of the Northern Ireland Department of Health Social Services and Public Safety

Dr Colin M Harper

September 2007

Contents

Summary

Introduction

It is clearly recognised in the DHSSPS Consultation on 'Protecting Personal Information' (2002) that there are problems with current practice in using service user information for secondary purposes. These problems are in terms of its legality and ethical basis. The key question then is whether something like Section 60 of the Health and Social Care Act 2001 is the best way to deal with this current anomaly.

There was no consensus in the responses in the Consultation as to how secondary uses should be addressed.

There will need to be both a new legal basis for the use of health and social information and there will need to be adjustments made to current practice to achieve greater compliance with human rights standards and law.

The common law on confidentiality

Whilst they interact in complex ways, it is important to recognize that the DAP98, HRA98 and the common law contain distinct obligations and meeting the obligations of one does not guarantee that one has met the obligations of another.

A breach of confidentiality in the legal sense would traditionally only arise where the following three conditions are fulfilled:

1) where the information has the necessary quality of confidence, i.e. it is private and is not in the public domain
2) where the information was imparted in circumstances that create an obligation of confidence (for example, in the context of the relationship between a member of health and social care staff and service user relationship)
3) where unauthorised use of the information would have a detrimental effect on the patient.

There is not a clear basis in these terms covering many current secondary uses of service user information.

The problem which section 60 was created to address was that information use and disclosure was taking place within the NHS for secondary purposes without a statutory basis, without the consent of patients and without a clearly recognized public interest which would override the public interest in maintaining confidences. Section 60 effectively constitutes a fourth item on the above list.

Section 60 of the Health and Social Care Act 2001

The purpose of Section 60 of the Health and Social Care Act is to allow organisations to obtain patient identifiable information, for medical purposes, in circumstances where it is impracticable to obtain informed consent from the patients concerned.

Section 60 is often described as being set up to address the problem of lack of patient *consent* to secondary uses, but the problem it tackles is lack of *any* of the three possible justifications for a breach of confidence.

The Patient Information Advisory Group (PIAG) was established under Section 61 of the Health and Social Care Act 2001 to advise the Secretary of State for Health about issues relating to the use of patient information. PIAG's role is to provide legal support for certain uses and disclosures of confidential healthcare information to continue whilst also acting as a catalyst to improve practice. This legal support is provided under Section 60 of the Health and Social Care Act 2001 and is granted through an application process. Applications are granted subject to certain conditions being met.

Secondary uses of health and social care information and data protection law

Any use or disclosure of heath and social care information under Section 60 or any equivalent measure must conform to the requirements of the Data Protection Act 1998.

Social care purposes are clearly not 'medical purposes' as defined in the DPA98 and thus condition 8 in Schedule 3 of DPA98 does not apply to them. It is possible that any Section 60 style arrangements which do not require explicit consent for secondary uses which are for social care purposes would fail to meet the requirements of the DAP98.

Information provided to service users should be sufficient to allow them to exercise their rights in relation to their data under the Data Protection Act 1998. It is clear that the above requirement is not being met with respect to secondary uses of service user information. It will need to do so for any Section 60 style measure.

If the safeguard conditions for the research exemption are met, then: personal data may be used for research even if not originally collected for that purpose; personal data may be retained indefinitely for the purposes of research; and subject access to the data may be withheld.

Secondary uses of health and social care information and human rights law

Secondary uses of information gathered from service users engages the human right to 'private life' which is protected by both the European Convention on Human Rights (ECHR) and the Human Rights Act 1998. The concept of "private life" covers: the physical and psychological integrity of a person; aspects of an individual's physical and social identity; gender identification, name and sexual orientation; personal

development, and the right to establish and develop relationships with other human beings and the outside world. The European Court of Human Rights also considers that the notion of personal autonomy is an important principle underlying the interpretation of the guarantees of Article 8 of the ECHR. Elements of 'private life', namely moral and mental integrity, clearly suggest that article 8 of the ECHR can be engaged even where service user information has been anonymised.

The European Court of Human Rights might take an interpretative approach which effectively sees the narrower range of limitations of the Biomedicine Convention as being those which are most appropriately limiting on the right to private life in the use of health and social care information.

As the protection of the privacy of health and social care information lies at the heart of the right to private life, any Section 60 style measure would have to pass a strong test of its proportionality. Any use would be required to have the minimum possible impact on privacy. There would have to be close and effective scrutiny of the measure. There would have to be a means for individuals to be heard.

There does not appear to have been a case at the ECtHR on the secondary use of health and social care information, but other relevant cases suggest that current practice may fall well short of what the Court would expect in terms of respect for private life.

Implications for a way forward for Northern Ireland?

Two key means for the protection of the interests of service users and ensuring that their moral and legal rights are respected are (1) anonymisation of information and (2) only using information with consent. Such measures are important to both meet legal requirements and to build the trust of service users in the health and social care system.

Whilst being important means of ensuring respect for the right to private life, gaining the consent of service users or offering an opt-out are not necessarily sufficient to ensure that this right is being respected.

Anonymisation should be pursued as an important means of protecting the right to private life and of ensuring the proportionality of any measure, but it does not remove completely the use of information from the protections of human rights law.

Any PIAG-style committee should be independent in the sense of not being made up of a majority of those who have an interest in using service user information. An independent appointments process and lay representation are both necessary. Any PIAG-style procedure for making decisions about the legitimacy of secondary uses should be compulsory and any guidance issued by such a body should be binding.

A general principle governing secondary uses of confidential service user information should be that the overriding of the common law obligation of confidentiality is a matter for legislators, not for regulators. Consideration should thus be given to a consolidating law to clarify the legal situation relating to health and social care information.

1. Introduction

As part of its work, the Privacy Advisory Committee of the Department of Health, Social Services and Public Safety (DHSSPS) is examining the possible need for and implications of Northern Ireland enacting an equivalent to S60 of the Health and Social Care Act 2001. This Report was commissioned to assist the Committee in its deliberations.

It examines the legal basis for the use and disclosure of information for purposes of health and social care which are not directly related to care of the service user from whom the information is obtained (secondary uses). Some potential and actual uses and disclosures of service user information are for purposes of health and social care but do not aim at the care of an individual service user. Many uses of service user information are increasingly required for evidence based practice and for a rational approach to health and social care service provision. The following are examples of such secondary uses: planning; financial management; commissioning; risk management; investigating complaints; auditing accounts; teaching; health and social care research; public health monitoring; registries; infectious disease reporting. It is not concerned about the use or disclosure of information for the care of that service user.

Concerns about lack of clarity around the legal basis for the secondary use of patient information in England and Wales were addressed through sections 60 and 61of the Health and Social Care Act 2001. This report looks critically at the approach adopted in England and Wales and attempts to articulate an appropriately balanced approach to the issues as a way forward for Northern Ireland.

The legal basis for secondary uses of the personal information of service users remain a much debated subject with widely diverging views on the justifications and bases for such use.[1] The debate often seems to separate into two camps with little common ground being found between the main positions adopted. On the one side are those who cannot understand that anyone could reasonably object to secondary or even research uses of information about their health and social care and that therefore such uses should be generally permitted. On the other side are those who would claim an absolute right to privacy and think that they are justified in using such a right to refuse any and all secondary and research uses of information obtained from them. An approach is necessary which recognises and protects the rights of individual service users yet facilitates important secondary uses in a proportionate way given those rights.

In the search for such a balance, it is sometimes argued that the current situation is 'unbalanced' largely due to two pieces of law in particular: the Human Rights Act 1998 (HRA98) and the Data Protection Act 1998 (DPA98). Both of these Acts have their ultimate origin in European law and are sometimes seen as 'foreign' to the UK and obstructive to the best practice developed here over the lifetime of the NHS. One

[1] See Academy of Medical Sciences, *Personal data for public good: using health information in medical research—Report of proceedings at the legal symposium* (June 2006). Although focused on research, this Report is a useful overview of many of contrasting views the legal issues which arise in connection with secondary uses.

side of the argument tends to see these requirements as needing amendment or replacement by a more 'balanced' approach. However, the 'European' origin of these laws makes it unrealistic to expect any amendment or change to their provisions as to do so would require agreed changes at a European level which are both unlikely to be secured and would take a long time to be implemented. Rather than being one side of the argument, the data protection law and relevant human rights law must be seen as the framework within which the debate must take place. Human rights constraints in particular set limits to the kinds of approaches which are open to addressing issues of the secondary uses. With its emphasis on privacy as a fundamental yet limited right, the human rights framework already provides the kind of balanced approach that is needed for secondary uses of health and social care information .

Debates on the secondary and research use of service user information often focus on data protection law and look to other EU countries for alternative models of how such uses can take place on a clear legal basis. However, whilst the requirements of data protection aw are undoubtedly important, they are relatively 'fixed' and the legal situation in other EU states is in general much simpler because they are civil rather than common law jurisdictions.[2] Whilst different approaches are adopted in different European states, none of them need a Section 60 equivalent as none of them have a common law obligation of confidentiality. (Other legal instruments such as statutes and constitutional provisions tend to cover similar issues to those addressed by the common law in the UK.) There is thus a risk in drawing comparisons with practice in other European states when their solutions cannot realistically be seen to address the challenges of the legal environment which were felt to make Section 60 necessary in the first place. The inescapable European context to the regulation of secondary uses can also be seen in that Section 60 was introduced to address issues created by the common law. It does not alter obligations under the Data Protection and Human Rights Acts which still apply. A more useful comparison for issues around Section 60 would be with other common law jurisdictions. They are not subject to the same data protection and human rights law requirements, so caution is required in such comparisons being drawn upon in attempting to formulate a model for Northern Ireland or indeed for the UK as a whole.

Northern Ireland is a society with a strong human rights culture and a relatively high level of awareness of human rights and a willingness to claim them. Through the work of the NI Human Rights Commission, all legal and policy measures are subject to greater scrutiny from a human rights perspective than in the other UK jurisdictions. In a world in which privacy seems continually undermined from various forces, it is important that any new arrangements work to build service user confidence in the handling of their private information by health and social care services. Any new provisions should form part of a comprehensive package of measures designed to increase protection for the privacy rights of service users whilst at the same time providing a legitimate basis for uses and disclosures essential for the provision of health and social care.

---

[2] See the website of the PRIVIREAL project (www.privireal.org) for much comparative material and also two of the publications emanating from that project: D. Beyleveld, D. Townend, S. Rouille-Mirza & J. Wright, *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, (Ashgate, 2004) & D. Beyleveld, D. Townend, S. Rouille-Mirza & J. Wright, *The Data Protection Directive and Medical Research Across Europe*, (Ashgate, 2005).

After some background in this introduction, the Report will consider the following issues. What is the common law on confidentiality? What is Section 60 of the Health and Social Care Act 2001? Secondary uses of health and social care information and data protection law. Secondary uses of health and social care information and human rights law. A possible way forward for Northern Ireland.

Previous HPSS Guidance and the Results of the Consultation

In *The Protection and Use of Patient and Client Information: Guidance for the HPSS*[3] the reality of secondary uses was clearly recognised:

> 1.2 It is in everyone's interests that the HPSS functions efficiently and effectively and makes best use of the resources available to it. To that end personal information about patients and clients is not only essential for the prime task of delivering personal care and treatment. It is necessary for a number of other purposes:
>
> i. assuring and improving the quality of care and treatment (*eg* through clinical audit);
> ii. monitoring and protecting public health;
> iii. coordinating HPSS care with that of other agencies (*eg* voluntary and independent services);
> iv. effective health and social care administration, in particular:
> - managing and planning services;
> - contracting for HPSS services, including the payment of staff, independent
> contractors and health and social service units for services and the authorization of extra-contractual referrals;
> - auditing HPSS accounts (including fraud investigation/detection and the work of external auditors appointed by HPSS Health Service Audit) and accounting for HPSS performance;
> - risk management (e.g. health and safety);
> - investigating complaints and notified or potential legal claims;
> v. teaching;
> vi. statistical analysis and medical or health and social services research to support
> (i)-(v) above.

However, the overall tone of this Guidance was one of protecting essentially the data protection rights of patients and clients through HPSS procedures. That service users have a human right to privacy which might set limits on those procedures does not feature significantly. Similarly, the nature and significance of common law obligations of confidentiality were underplayed. There are two aspects to the approach in the Guidance that are cause for concern:

---

[3] *The Protection and Use of Patient and Client Information: Guidance for the HPSS* (1999?). A new *Code of Practice on Protecting the Confidentiality of Service User Information* is currently being consulted upon.

- the obligations of the DPA98 are discussed as if they are almost the only ones that staff need be concerned about when in fact the obligations of the common law and human rights law are much more onerous;
- the use of 'implied consent' as a basis for the use and disclosure of information is stretched beyond its legal limits—often it seems to be deployed as a mantra to evade obligations, rather than in any convincing way as a clear means though which obligations are met.

A consultation paper was circulated in June 2002[4] which identified the 'current problems':

> 3.1 It is clear that the HPSS (together with the NHS in England and Wales and NHS Scotland) does not fully comply with the fair and lawful processing requirement of the DPA98 and the Common Law. Instead it relies, by default, on the implied consent of service users for the processing of much, if not all, personal information. HPSS bodies, therefore, risk legal challenge due to breach of the DPA98. Implied consent is based on the assumption that service users are aware of, and understand, all the uses HPSS bodies make of their personal information. However, because of the lack of transparency, service users are largely unaware of how their personal information is used, beyond the provision of direct care and treatment. Implied consent is, therefore, unlikely to be valid for all the uses of personal information at present.
> 3.2 It is, however, important to ensure that actions by HPSS bodies to comply with current legislation do not restrict or inhibit the benefits which flow from the sharing of information. HPSS bodies need to move to a position where they can comply with current legislation, professional guidance and best practice without unnecessary restriction to essential information flows. This will involve HPSS bodies changing the way they currently deal with service users and use their personal information. In order to do this the following is considered essential:
>
> i. service users must be informed about how information about them is used, by whom and for what purposes;
> ii. personal data should be anonymised wherever possible;
> iii. if data cannot be anonymised to an acceptable degree service users must give informed consent; and
> iv. the need for new legislation should be considered.

These concerns and 'solutions' clearly mirror those which arose in England and Wales and lay behind the adoption of Section 60, in particular in the requirement for informed consent. In both the Consultation paper and the responses to it[5] there was a lot of confusion, particularly around the notion of 'implied consent'. It is worth quoting the consultation response on the case for legislation:

> 2.10 There was no consensus on the question of whether legislation, similar to section 60 of the Health and Social Care Act 2001 to override the duty of confidence, should be introduced, and if so, whether it should be permanent or temporary.

---

[4] *Health and Personal Social Services. Protecting Personal Information: A Consultation Paper* (DHSSPS: June, 2002).
[5] *Health and Personal Social Services. Protecting Personal Information: Responses to a Consultation Paper* (DHSSPS: March, 2003).

It was suggested that information relating to :-

- public health information;
- cerebral palsy;
- communicable disease;
- the Cancer Registry;
- diabetes;
- congenital anomalies;
- accidents;
- heart disease and stroke;
- diagnosis and conditions which are major causes of death
- and morbidity;
- National Joint Registry for Orthopaedics;

should be included in any legislation which is introduced.

However some respondents said that legislation would not be necessary for cancer registries if cancer were to become a notifiable disease.

A number of responses stated that information which is not relevant to the direct care of the patient, but which is of importance for the overall management of health and social care should be included in legislation. Other more specifically cited information relating to probity, planning, targeting of resources and audit. Some concern was expressed that retrospective legislation would be practically difficult, and expensive to implement. Others thought that there should be retrospective legislation to deal with existing records.

Although it states that 'no consensus on the question of whether legislation, similar to section 60 of the Health and Social Care Act 2001 to override the duty of confidence, should be introduced', the arguments against such legislation are not presented as clearly as the arguments in its favour.

A specific question was asked in the Consultation on the case for legislation:

The Consultation Paper said: "The main arguments in favour of legislation are in relation to the greater good, probity and data quality (Paragraph 3.27) and the main argument against legislation is the infringement of the right to privacy" (Paragraph 3.28)

The Consultation Paper asked, "Is there a need for legislation here similar to section 60 to override the duty of confidence? If so, should it be temporary or permanent?"

The responses said

yes
no
permanent
temporary
temporary, then reviewed, then made permanent
Legislation would not be necessary for cancer registries for example if cancer was to become a notifiable disease

No information is provided as to how common each of these responses was, so it is difficult to judge much about the views of staff and the public from this. It does suffice to demonstrates that there is not agreement and that any legislative proposal is likely to be contentious. A further question about 'which information flows should be included' produced the following list of responses:

- Information flows relating to public health
- Communicable diseases
- Information flows to Cancer Registry, National Joint Registry for Orthopaedics and for financial audits
- Diabetes
- Cerebral palsy
- All cancers and pre-cancerous conditions
- Congenital anomalies
- Accidents, heart disease, stroke
- Diagnosis and conditions which are major causes of death and morbidity Information flows which are not relevant to the direct care of the patient but which are of importance for the overall management of health and social care
- Probity, planning, targeting

There was no consensus in the responses in the Consultation as to how secondary uses should be addressed.

Two approaches suggest themselves:

1. Adjust the law to make current practice legal

2. Adjust current practice to make it conform to the legal framework as it stands.

In reality, the best approach will probably require an element of both of these. There will need to be both a new legal basis for the use of health and social information and there will need to be adjustments made to current practice to achieve greater compliance with human rights standards and law.

Summary

It is clearly recognised in the Consultation that there is a problem with current practice in terms of its legality. The question then is whether something like Section 60 of the Health and Social Care Act 2001 is the best way to deal with this anomaly.

There was no consensus in the responses in the Consultation as to how secondary uses should be addressed.

There will need to be both a new legal basis for the use of health and social information and there will need to be adjustments made to current practice to achieve greater compliance with human rights standards and law.

2. The common law on confidentiality

The common law is the law that develops over time through the decisions of judges in particular cases. As such it is perhaps less clear at times than law which is created by statute, but many common law concepts are quite clear and have developed over a long period. The common law changes with new judgments, but it can also be stable over long periods.

One of the problems with discussions about the use and disclosure of health information is the possible meanings of 'confidential'. Something can be confidential in different ways. It is not always the legal sense that is meant when it is used in discussions about health and social care information. For example, the *Draft Code of Practice on Protecting the Confidentiality of Service User Information* uses the word in a more general sense in its title and then discusses the particular common law meaning within an appendix. As well as having a legal meaning, 'confidentiality' is also an ethical concept. Ethical obligations in this respect may differ from the legal obligations and may also differ depending on their source. For example: a natural right to privacy; an aspect of 'good conduct' as defined by statutory regulators such as the Northern Ireland Social Care Council; or as defined by international professional organisations such as the World Medical Association.

The legal sense of 'confidential' is narrower than the everyday use of the term as a synonym for 'private' or 'secret'. Something is not confidential in the legal sense simply because it is marked as such. A breach of confidentiality in the legal sense would traditionally only arise where the following three conditions are fulfilled:

1) where the information has the necessary quality of confidence, i.e. it is private and is not in the public domain
2) where the information was imparted in circumstances that create an obligation of confidence (for example, in the context of the relationship between a member of health and social care staff and service user relationship)
3) where unauthorised use of the information would have a detrimental effect on the patient.

It is questionable whether the third criterion above is essential as it is possible for a breach of confidence to occur where information is disclosed which portrays a person in a positive light. It is probably unsafe to assume that where there is no harm to a service user, there cannot be a breach of confidence.

It is important to distinguish between having a general duty to maintain confidentiality and having a particular obligation with respect to particular information. It is sometimes suggested that it makes a difference when a disclosure is made to another health and social care professional who is also under a duty of confidentiality.[6] Even provided that high standards of confidentiality are maintained, a legal breach can still have occurred. Whilst that someone owes 'a duty of confidentiality which is equivalent' may be significant in terms of the DPA98, it does

[6] See for example, Confidentiality and Security Advisory Group Scotland, *Protecting Patient Confidentiality: Final Report*, (2002).

not suffice to warrant disclosure of confidential information in terms of the common law. If a service user makes a disclosure to a member of staff, a further disclosure is still a breach of a particular confidentiality obligation even though the person to whom the member of staff makes the disclosure is themselves under a general obligation of confidence.

The common law on confidentiality provides a large measure of *control* to the service user over the flow of information. If a service user discloses information to someone in such a way that it is confidential, then that person is not meeting their common law obligations if they disclose it to someone else even though that person is under some general 'obligation of confidence'.

However, making such a disclosure may mean that the person to whom the information is disclosed *acquires* an obligation of confidence with respect to it.

A disclosure of confidential information may be justified in the common law in one of three ways:

1. the service user has given a *valid consent* (which can be express or implied);
2. a public interest overrides the public interest in confidentiality in a particular situation; or
3. a statutory basis exists which permits or requires disclosure.

The existence of one of these three does not completely remove the obligation, but rather provides a justification for a breach of the obligation. Recent case law involving the right to privacy and the media has extended the applicability of the obligation of confidence to include situations where there is no pre-existing relationship between the parties in which the information was confided. The law on confidentiality is therefore now broader in that it can be used more generally to protect against the misuse of one's personal information.

Whist they interact in complex ways, it is important to recognize that the DAP98, HRA98 and the common law contain distinct obligations and meeting the obligations of one does not guarantee that one has met the obligations of another. That the processing of personal data is taking place in keeping with the requirements of the DPA98 and the HRA98 does not mean that no breach of the common law of confidence is occurring.

The level of protection offered by the common law is quite high in principle, although the extent to which service users can effectively enforce those legal protections in practice is a different matter. It is also the case that once confidentiality has been breached, no legally remedy can effectively restore the situation before the breach.

The problem which section 60 was created to address was that information use and disclosure was taking place within the NHS for secondary purposes without a statutory basis, without the consent of patients and without a clearly recognized public interest which would override the public interest in maintaining confidences. The nature and functioning of section 60 is considered in the next chapter.

Summary

Whilst they interact in complex ways, it is important to recognize that the DAP98, HRA98 and the common law contain distinct obligations and meeting the obligations of one does not guarantee that one has met the obligations of another.

A breach of confidentiality in the legal sense would traditionally only arise where the following three conditions are fulfilled:

4) where the information has the necessary quality of confidence, i.e. it is private and is not in the public domain
5) where the information was imparted in circumstances that create an obligation of confidence (for example, in the context of the relationship between a member of health and social care staff and service user relationship)
6) where unauthorised use of the information would have a detrimental effect on the patient.

There is not a clear basis in these terms covering many current secondary uses of service user information.

The problem which section 60 was created to address was that information use and disclosure was taking place within the NHS for secondary purposes without a statutory basis, without the consent of patients and without a clearly recognized public interest which would override the public interest in maintaining confidences. Section 60 effectively constitutes a fourth item on the above list.

3. Section 60 of the Health and Social Care Act 2001

Background

Section 60 of the Health and Social Care Act 2001 was introduced in England and Wales to deal with the problems around the use of confidential patient information for healthcare purposes that have been identified above. The purpose of section 60 has been described as follows:

> The purpose of Section 60 of the Health and Social Care Act is to allow organisations to obtain patient identifiable information, for medical purposes, in circumstances where it is impracticable to obtain informed consent from the patients concerned. Section 60 is intended to be transitional, allowing the NHS time to develop procedures for obtaining consent from patients or find ways of working with pseudonymised/anonymised information.[7]

Section 60 is often described as being set up to address the problem of lack of patient *consent* to secondary uses, but the problem it tackles is lack of *any* of the three possible justifications for a breach of confidence. The purpose of the section as described above emphasises the importance of gaining consent as the normal and main route for using information for secondary purposes, but this is a policy goal rather than a strict legal requirement.

Implementing Section 60

The Patient Information Advisory Group (PIAG) was established under section 61 of the Health and Social Care Act 2001 to advise the Secretary of State for Health about issues relating to the use of patient information. PIAG's role is to provide legal support for certain uses and disclosures of confidential healthcare information to continue whilst also acting as a catalyst to improve practice. This legal support is provided under Section 60 of the Health and Social Care Act 2001 (see Annex 1) and is granted through an application process. The body to which application must be made is the Patient Information Advisory Group.

Terms of Reference of the Patient Information Advisory Group

Advise the Secretary of State for Health on use of powers provided by Section 60 of the
Health and Social Care Act 2001, and in particular on:
- Applications and proposals for use of these powers;
- Draft regulations made under s60(1) of the Act;
- Proposals to vary or revoke such regulations following the Secretary of State's required annual review of existing provisions.

Advise the Secretary of State on key issues, particularly those of national significance,
relating to the processing of patient information.

[7] See the website of the Patient Information Advisory Group (PIAG): http://www.advisorybodies.doh.gov.uk/piag/ Much of the basic information about PIAG presented here is taken from its website.

A statute or statures could have been created which would make legal certain specified uses of information which was held in confidence in the common law sense. However, Section 60 goes beyond this in creating the possibility of ongoing decision-making about the lawfulness of such uses outside of primary legislation. Section 60 effectively creates a fourth possible basis for a breach of confidence alongside consent, statute and the existence of a public interest which overrides the public interest in confidentiality. 'Section 60 support' thus makes legal what would otherwise be illegal at common law. It does not modify data protection obligations nor does it remove the requirements of human rights law.

PIAG has identified 'key principles' which it considers are necessary for Section 60 support to be granted. (See below.)

Key Principles of PIAG for Section 60 support

- Where an organisation has a direct relationship with a patient then it should be aiming to obtain consent.
- Consent should be sought by clinicians who have a direct relationship with patients.
- Organisations should not hold data on patients who specifically refuse consent.
- Section 60 support cannot be used to over-ride dissent of patients who do not wish to take part in research studies
- "Third Party" organisations should be seeking to use anonymised/pseudonymised data.
- The NHS number should be used wherever possible.
- All organisations seeking Section 60 support should build patient/service user involvement into their processes.
- All organisations with Section 60 support should make information materials available to patients describing the information they use and why they need it.
- In certain studies, for example, where small numbers are involved, a 100% sample may be necessary but PIAG does not accept that 100% samples are essential in all research studies.
- Organisations need to recognise that Section 60 is an interim measure and therefore
need to develop an exit strategy from needing S60 support, either through the National Programme for Information Technology's Secondary Uses Service or by obtaining consent.
- Research carried out with Section 60 support must be significant in terms of subject matter and scale and must be likely to benefit the patients concerned or the wider public.

Any application for support under Section 60 of the Health and Social Care Act 2001 must ensure that it is using data for a medical purpose defined as acceptable under the Act.

According to the Act "medical purposes" means the purposes of any of the following:

(a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services, and

(b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care or treatment;

PIAG has made it clear that it does not see its task as making it easier for use to be made of confidential information. It has a strong focus on getting organisations to rely on consent where this could be obtained and to anonymise information as much as possible.

An additional requirement is that: 'Organisations and individuals seeking Section 60 support must also present a robust case to demonstrate that the use of patient identifiable information is in the best interests of patients or, alternatively, serves a wider public good of sufficient merit to warrant the risk to confidentiality.

Regulations made under Section 60 provide either *specific* or *class* support for the use of confidential information.

Specific Support applies to particular activities that have been approved by Parliament. To date, Parliament has approved the use of Section 60 powers for two purposes: communicable disease surveillance and cancer registration.

Class Support applies to activities that can be approved by PIAG acting on the Secretary of State for Health's behalf. The Section 60 support available for work falling into this category is limited to one or more of the following purposes:
Class I: The process of anonymising patient records.
Class II: Analysis of geographical data.
Class III: Work to identify and contact patients in order to obtain their consent.
Class IV: Record linkage and validation.
Class V: Clinical audit and monitoring of healthcare provision.
Class VI: For one or more of the above purposes

Conditions of Section 60 Support
In providing section 60 support for particular use of confidential information, PIAG also has certain conditions attached to such uses which it checks an organisation can fulfill and is fulfilling. These conditions 'flesh out' the 'key principles for section 60 support' and are set out in the box below.

PIAG Conditions for Section 60 Support:

We require that organisations provide evidence that:
• All staff with access to the patient identifiable information have contractual obligations of confidentiality, enforceable via disciplinary procedures.
• All staff with access to patient identifiable information have received appropriate training, receive ongoing supervision and support to ensure they are aware of their responsibilities and are able to deal with queries as they arise.
• They comply with the requirements of the Data Protection Act.
• They have implemented an appropriate IT security policy to protect and preserve the information.
• Access to patient identifiable information is limited to the minimum necessary to satisfy the purposes for which the information was made available.

• They will not disclose identifiable patient information except:
- to the data controller that made the information available;
- to other data controllers similarly supported in law for limited uses of data;
- to others on a need to know basis where there is a significant public health interest justification for doing so;
- where there is a specific statutory requirement to do so.
• Patient information will only be held in an identifiable form for the minimum time necessary.
• They will only process patient identifiers that are needed to satisfy the purposes for which Section 60 support was sought.
• They will document and make available to anyone who requests them, details of how the conditions set out in Section 60 are being met;
• They will facilitate and support reasonable audit of data processing by designated agents of the Secretary of State.

Once an application has been granted, PIAG has a process for undertaking an annual review of the need for section 60 support. In keeping with the idea that section 60 is a transitional measure, PIAG actively seeks evidence that organizations are moving towards informed consent or anonymisation/pseudonymisation. Where it is claimed that either of these two options remain impracticable, then evidence is sought for how this claim has been tested or how attempts have been made to develop alternative ways of working which do not require confidential information.

Summary

The purpose of Section 60 of the Health and Social Care Act is to allow organisations to obtain patient identifiable information, for medical purposes, in circumstances where it is impracticable to obtain informed consent from the patients concerned.

Section 60 is often described as being set up to address the problem of lack of patient *consent* to secondary uses, but the problem it tackles is lack of *any* of the three possible justifications for a breach of confidence.

The Patient Information Advisory Group (PIAG) was established under Section 61 of the Health and Social Care Act 2001 to advise the Secretary of State for Health about issues relating to the use of patient information. PIAG's role is to provide legal support for certain uses and disclosures of confidential healthcare information to continue whilst also acting as a catalyst to improve practice. This legal support is provided under Section 60 of the Health and Social Care Act 2001 and is granted through an application process. Applications are granted subject to certain conditions being met.

4. Secondary uses of health and social care information and data protection law

Any use or disclosure of heath and social care information under Section 60 or any equivalent measure must conform with the requirements of the Data Protection Act 1998. The Data Protection Act 1998 (DPA98) gives effect in UK law to '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 aim of the Directive and thus of the DPA98 is to protect the rights of people in respect of the processing of personal data; not only their privacy rights, but all their fundamental rights insofar as they might be affected by such data processing.

As its source is EU law, the DAP98 must implement the requirements of the Directive and the DPA98 thus cannot be modified unless the Directive were to be modified.[8] Thus any Section 60 equivalent will always have to be compatible with the DAP98 insofar as it is compatible with the Directive.

The DPA98 defines 'personal data' as data 'which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.' The Act thus only applies to data which relate to a living person and it does not apply to data which has been anonymised. That is, the Act only applies where an individual 'can be identified (a) from those data, or (b) from those data and other information which is in the possession of or likely to come into the possession of, the data controller'. In this respect the data protection law differs from the human rights law and there seems to be nothing in the human rights case law to suggest that anonynised information cannot impact on the right to private life as understood in the ECHR.

Meeting Schedule 3 Conditions

The DPA98 introduces eight 'Data Protection Principles' that set out standards of information handling. The First Data Protection Principle states:

> "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -
> a) at least one of the conditions in Schedule 2 is met, and
> b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

In the context of data controllers in health and social care, the most relevant Schedule 2 conditions are likely to be:

---

[8] It has been argued that the DPA98 currently inadequately implements the Directive, in which case the Act could be modified in order to bring it in to line. The arguments along this line generally suggest that the DPA98 fails to provide sufficient protection for personal data. If true, this would likely make it even more difficult for section 60 style arrangements. I assume here that the Act does implement the Directive adequately.

1. Processing with the consent of the data subject;
4. Processing necessary to protect the vital interests of the data subject;
5. Processing which is necessary for the exercise of functions of a public nature exercised in the public interest by any person;
6. Processing which is necessary for the purposes of the legitimate interests pursued by the data controller or those of a third party to whom the data are disclosed, except where the processing is prejudicial to the rights and freedoms or legitimate interests of the data subject.

'Sensitive personal data' attracts significant additional protection and is further defined in the DPA98 to mean personal data consisting of information as to-

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The most relevant Schedule 3 conditions to health and social care are likely to be:

1. Processing with the explicit consent of the data subject;
3. Processing necessary to protect the vital interests of the data subject or another person, where it is not possible to get consent;
6. Processing necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
8. (1) The processing is necessary for medical purposes and is undertaken by: (a) a health professional, or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

'Medical purposes' is defined quite broadly in the DPA98 and in *health* care this is possibly the most likely basis for the processing of sensitive personal data for secondary purposes. Explicit consent is not therefore required for the processing of sensitive personal data for 'purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services'.

In the guidance on health data from the Information Commissioner[9], it is suggested that, as for care and treatment, the Schedule 3 condition for a wide range of secondary uses is likely to be Condition 8. The guidance explicitly refers to the

[9] Information Commissioner's Office, *Use and Disclosure of Health Data*, (May, 2002).

following as examples of uses and disclosures likely to be dependent upon Condition 8:

- Processing for administrative purposes
- Administrative audit
- Statutory disclosures to disease registries or statutory disclosures for epidemiological research
- Non-statutory disclosures to disease registries or non-statutory disclosures for epidemiological research
- Clinical trials
- Teaching

Social care workers would come under 'a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional'. However, a major problem arises in connection with social care in that social care purposes are clearly not 'medical purposes' as defined in the DPA98 and thus condition 8 in Schedule 3 of DPA98 does not apply to them. It is not clear from the Department of Health's guidance on the DPA98 for social services as to what it considers the likely Schedule 3 condition to be for secondary uses of personal information. It lists 'relevant conditions' from Schedule 2, but not from Schedule 3.[10] It therefore is likely that any Section 60 style arrangements which do not require explicit consent for secondary uses which are for social care purposes would fall foul of the DAP98 (in not providing a Schedule 3 condition for the processing of sensitive personal data). It may be the case that the integrated nature of health and social services in Northern Ireland means that Section 60 style arrangements could not be practically implemented. Anonymisation with explicit consent for that anonymisation may be the only viable route for secondary uses for social care purposes.

Providing Information to Service Users

The Information Commissioner has issued guidance on how much information it is necessary to provide to service users to meet the requirements of the DPA98. The key point is that the information provided should provide sufficient information to allow service users to exercise their rights in relation to their data under the Act.

> They should be told who will process their data, including any disclosures of personal data (which will allow them to make subject access requests), whether it must be supplied (which will allow them to opt-out if they wish), and what information is contained in their record (which will allow them to give meaningful consent to its processing.) It should provide sufficient information to allow the individual to assess the risks to him or her in providing their data, in consenting to their wider use, in choosing not to object to their processing etc. This should have at least two consequences for data controllers. It should become clear that fair processing notices do not need to contain a large amount of detail about routine, administrative uses of data.[11]

[10] See *Data Protection Act 1998: Guidance to Social Services*, (Department of Health, March 2000). See particularly pp. 36-37 on 'Disclosure without consent' and 'Social services purposes'.
[11] Information Commissioner's Office, *Use and Disclosure of Health Data*, (May, 2002).

It is clear that the above requirement is not being met with respect to secondary uses of service user information within DHSSPS. This is unquestionably an area where practice will have to change to conform to the law as the source of the DPA98 in European Law means that the DPA98 cannot be changed (assuming that it is an effective implementation of the EU Data Protection Directive) .

The Exemption for Research

Secondary uses of personal information which constitute 'research' may be exempt from certain provisions of the DPA98 under Section 33 of the Act. The data processing concerned must be 'only for research purposes'. 'Research' is not defined in the Act but it is stated that it specifically includes 'statistical and historical purposes'. The research exemptions concern the following provisions of the DPA98:

(a) The second Data Protection Principle (data must not be processed in a manner which is incompatible with purpose for which it was obtained)

(b) The fifth Data Protection Principle (data cannot be kept indefinitely)

(c) The subject access provisions (right of data subject to see personal data held on them) where 'the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them'.

These exemptions only apply where certain conditions are met, namely:

(1) 'that the data are not processed to support measures or decisions with respect to particular individuals';

(2) 'that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject'.

The research exemption is of limited relevance and value when it comes to processing for secondary uses. Although much audit activity could be characterised as 'research', there is perhaps a tendency not to do so as it would engage research governance procedures, including the need for approval by a research ethics committee and a possible requirement for informed consent. Audit is also likely to be processing 'to support measures or decisions with respect to particular individuals'. Where the secondary use is 'health and social care research', then care would need to be taken to ensure that particular service users are not implicated in decision which may flow directly from the research conducted using their information. This does not preclude a flow back of benefit to service users. For example, research which generates new policies or procedures can be implemented to the benefit of service users, including those whose information was used. However, it probably must be of general benefit and have been envisaged as potentially being so in order to meet condition (2) above.

Summary

Any use or disclosure of heath and social care information under Section 60 or any equivalent measure must conform to the requirements of the Data Protection Act 1998.

Social care purposes are clearly not 'medical purposes' as defined in the DPA98 and thus condition 8 in Schedule 3 of DPA98 does not apply to them. It is possible that any Section 60 style arrangements which do not require explicit consent for secondary uses which are for social care purposes would fail to meet the requirements of the DAP98.

Information provided to service users should be sufficient to allow them to exercise their rights in relation to their data under the Data Protection Act 1998. It is clear that the above requirement is not being met with respect to secondary uses of service user information. It will need to do so for any Section 60 style measure.

If the safeguard conditions for the research exemption are met, then: personal data may be used for research even if not originally collected for that purpose; personal data may be retained indefinitely for the purposes of research; and subject access to the data may be withheld.

5. Secondary uses of health and social care information and human rights law

When the privacy of service users is being discussed, a general notion is often used. This differs markedly from how 'privacy' has developed as a concept of human rights law. 'Privacy' or 'private life' in human rights law is a broader concept than the general concept. A lack of domestic or European cases directly on the issue of secondary uses means that the likely approach of the courts must be constructed from other cases involving health and social care information, from other human rights instruments which are likely to be persuasive and from general principles of human rights law such as 'proportionality'.

The Council of Europe's *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR) is an international treaty which is binding on all those states that have ratified it, which includes all members of the European Union. The Human Rights Act 1998 (HRA98) incorporates most of the European Convention on Human rights into the domestic law of the UK. Before this anyone who thought their rights under the Convention had been violated had to make a complaint to the European Court of Human Rights in Strasbourg (ECtHR), but under the HRA98 courts in the UK can enforce some of the rights contained in the Convention. It is still open to individuals to take a case to the ECtHR in Strasbourg once they have exhausted domestic remedies. It is unlawful for a public authority to act in a way that is incompatible with a right contained in the European Convention on Human Rights (ECHR) as set out in Schedule 1 to the Human Rights Act 1998. HSS Trusts are public bodies for this purpose and must ensure that Convention rights are not breached, both by the Trust and by its staff.

The article which is likely to be of most relevance to any Section 60 style arrangement is article 8. However, it does not exhaust the range of ECHR rights which might be engaged in through any Section 60 style measure, particularly if information gathered under a Section 60 type power were subsequently to be used for other purposes. After a discussion of the meaning of 'private life' in article 8 and the significance of the limitations of article 8 (2), and the nature of 'proportionality' in assessing limitations, consideration will be given to two leading cases of relevance.

There do not seem to be any cases which directly address the issues raised by secondary uses of personal information. However, there are two major cases which define the approach of the European Court of Human Rights to medial confidentiality in certain respects and these can be drawn on to identify the principles which the Court might adopt in any future consideration of secondary uses. A consideration of these principles is useful as it helps to inform how any new law should be framed to pre-empt legal challenge on human rights grounds.

ECHR Article 8

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms is of obvious relevance to the question of the issue of the rights of research subjects with respect to the use of their information. It reads as follows:

> Article 8 – Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 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.

Meaning of 'Private life' in Article 8 (1) of the ECHR

The concept of 'private life' is not easy to define, something which the court itself has recognised and also consistently refused to do. The only alternative is to develop an ostensive definition based on case material. It is by no means reasonable to assume that the total set of such cases would provide a coherent notion of 'private life', indeed it seems that the Court is almost keen to avoid too much definition in order to preserve flexibility in its application of this article of the Convention. It is particularly important to note how much broader the ECtHR view of privacy is than the limited everyday notion of 'privacy' which it also includes.

The Court recently reaffirmed its interpretation of the meaning of 'private life' in Pretty v the United Kingdom (2002):

> As the Court has had previous occasion to remark, the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person ... It can sometimes embrace aspects of an individual's physical and social identity ... Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 ... Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world ... Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.[12]

It is clear from these definitions of the scope of the right, that any secondary use of service user information will engage article 8 of the ECHR. That means that any such use must be justified in the light of the limitations on the right contained in article 8. It is also clear that elements of 'private life', namely moral and mental integrity, mean

[12] Pretty v the United Kingdom (Application no. 2346/02), Judgement of 29 April 2002, para. 61.

that article 8 can be engaged even where information has been anonymised. (See Appendix 4 for further detail on the nature of 'private life'.)

Limitations of Article 8 (2)

The only restrictions allowed on the rights contained in the Convention are those which actually specified in it—hence, in every case any restriction of Art. 8 (1) must be on the basis of satisfying the express criteria of Art. 8 (2). Any restriction of Art 8 (1) must:

(a) be in accordance with the law;
(b) be for a specified legitimate aim; and
(c) be necessary in a democratic society.

To be (a) in accordance with the law: it must be established that the interference with the Convention right has some basis in national law; the law must be accessible; the law must be formulated in such a way that a person can foresee the consequences that a given action will entail.

To be (b) for one of the specified legitimate aims, the limitation must serve at least one of the following aims which must be interpreted narrowly:

(1) in the interests of national security,
(2) in the interests of public safety,
(3) in the interests of the economic well-being of the country,
(4) for the prevention of disorder or crime,
(5) for the protection of health,
(6) for the protection of morals,
(7) for the protection of the rights and freedoms of others.

To be (c) necessary in a democratic society the interference must (i) correspond to a 'pressing social need' and (ii) be 'proportionate to the legitimate aim pursued'.

It is important that the list of 'limitations' in article 8 (2) are read as such—they are not competing interests which must be 'balanced' against the 'interest' in 'private life' contained in article 8 (1). They are not in themselves principles which compete with a principle of respect for 'privacy', but rather they are exceptions to the principle which must be interpreted narrowly. It can be misleading in terms of human rights law to think of competing 'public interests' within a particular Convention right—it is more appropriate to think of the right as a limit on the exercise of the public interest. In the case of article 8, this limit on the public interest is not absolute.

Another limitation of relevance is 'the protection of the rights and freedoms of others'. The potential key limitation in the context of secondary uses is that of 'the protection of *the right to health*' (as distinct from 'the protection of *health*' as a limitation of the right). The right to health is not a right guaranteed by the ECHR, but it is a clearly

recognised human right and it features as an obligation in Article 11 of the European Social Charter[13]:

> With a view to ensuring the effective exercise of the right to protection of health, the Contracting Parties undertake, either directly or in co-operation with public or private organisations, to take appropriate measures designed *inter alia*:
>
> 1 to remove as far as possible the causes of ill-health;

To 'remove the causes of ill-health as far as possible will necessarily mean the secondary use of private information provided by service users. Contracting Parties to the Social Charter are also committed to pursue the attainment of conditions in which the following principle is realised 'by all appropriate means': 'Everyone has the right to benefit from any measures enabling him to enjoy the highest possible standard of health attainable.' Clearly secondary uses are potentially such an 'appropriate means'.

It remains to be argued in particular cases whether a particular secondary use is 'necessary in a democratic society' in both respects of 'corresponding to a pressing social need' and being 'proportionate to the legitimate aim pursued'. There is no doubt of the 'pressing social need' for more effective, more efficient and more cost effective health and social care interventions—care costs in particular are huge and likely to increase dramatically given Europe's aging population. It is likely that speculative research would not be considered a legitimate aim by the Court. Judgments on proportionality would come down to the very particular circumstances of disclosure of information in particular cases, with there being very little scope for the articulation of general principles. Under Section 60 type arrangements challenges on the basis of proportionality might be made in two ways: (1) the proportionality of granting section 60 support to the particular kind of secondary use; (2) the proportionality of interfering with this person's right to private life in using their information.

In making any judgments concerning secondary uses the ECtHR is likely to look at other instruments of international human rights law for guidance on best practice. Although the 'Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine' (ECHRB)[14] has not been signed by the UK, it has been cited in domestic judgments as having persuasive authority. The ECtHR would almost certainly give significant weight to principles enshrined in this other Convention of the Council of Europe in deciding any case on secondary use of service user information.

Article 10 of the ECHRB is devoted to 'Private life and right to information':

> 1. Everyone has the right to respect for private life in relation to information about his or her health.

[13] Article 12 of the ICESCR also guarantees 'the right of everyone to the enjoyment of the highest attainable standard of physical and mental health'.
[14] See http://conventions.coe.int/treaty/en/treaties/html/164.htm.

2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.

3. In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

Article 26 of the Convention on Human Rights and Biomedicine lays out what restrictions can be placed upon some of the rights that the Convention contains.

1. No restrictions shall be placed on the exercise of the rights and protective provisions contained in this Convention other than such as are prescribed by law and are necessary in a democratic society in the interest of public safety, for the prevention of crime, for the protection of public health or for the protection of the rights and freedoms of others. ...

The restrictions contained in Article 26 (1) are thus very similar to those contained in Article 8 (2) of the ECHR (see below).

Possible Restrictions on Article 8/1 of ECHR	Possible Restrictions on Article 10/1 of ECHRB
in the interest of national security	
in the interest of public safety	in the interest of public safety
the economic well-being of the country	
the prevention of disorder or crime	the prevention of crime
the protection of health or morals	the protection of public health
the protection of the rights and freedoms of others	the protection of the rights and freedoms of others

Table One: Comparing Restrictions on Art. 8/1 of the ECHR and Article 10/1 of the ECHRB

Both Conventions require that the restrictions be 'in accordance with' (ECHR) or 'prescribed by' (ECHRB) law and be necessary in a democratic society. However, the 'interests of national security' and 'the economic well-being of the country' are absent in the ECHRB. It is also noteworthy that 'protection of health' is replaced by the significantly narrower 'protection of public health' and 'protection of morals' is also absent. In general this makes the ECHRB protection of privacy subject to significantly fewer limitations than the corresponding right is subject to in the ECHR. It could be argued that the narrower range of restrictions of the Biomedicine Convention are in fact those appropriate for health information and by extension for social care information when it is embedded with health information.

In particular, if the ECtHR were to come to see 'the economic well-being of the country' as not readily available for restricting the privacy of health information or was to see the text of the Biomedicine Convention as providing clear guidance on how economic considerations should be afforded little weight in reaching judgements of proportionality, then a key argument in favour of many secondary uses is potentially either removed or weakened. The removal of 'in the interest of national security' as a limitation would reassure many people that confidential information granted assess to

through PIAG style procedures could not be further disclosed for purposes of 'national security'.

Proportionality?

In human rights law questions of proportionality in terms of limiting a right are not simply ones of weighing one interest against another. The human rights test is more stringent than that traditionally applied by UK courts in that the presumption is that the Convention right should respected

To be compliant with human rights law, any Section 60 type arrangements and any support granted under them would have to be proportionate in this sense. Key elements in making such judgements include:

- Whether the interference impairs the 'essence' of a right. The greater the right interfered with, the greater the likelihood that there will be a breach of the Convention. The protection of intimate health and social care information disclosed by a person for their care and treatment is likely to be seen as lying at the heart of the Convention aim of protecting 'private life'.

- Whether a less restrictive alternative is available to achieve the aim pursued. This is where the PIAG approach of requiring pursuit of anonymisation is important as this would mean less restriction of the right to private life. Another key issue for Section 60 type arrangements is the way in which some measures mean *all* people have their right restricted. If it is possible to achieve the aim without infringing everyone's right, then not to do so might well be seen as disproportionate.

- Whether there are effective safeguards and legal controls over the measures, including legal remedies for those affected by the measures. This touches on the Section 60 requirement for PIAG approval. The question is whether such arrangements are indeed 'effective'. The make-up of any body with decision-making powers is crucial in assessing its likely effectiveness in protecting the rights of all service users. To be 'proportionate', the majority of any body with decision-making powers over peoples rights should probably be lay members and a member with expertise in human rights law be included. Recent trends in the expansion of the lay composition of statutory regulators in health and social care is also relevant here.

- A measure is more likely to be proportionate if there is an element of fairness to the person affected built into the measure. If the person affected was not consulted or given a right to a hearing, then there is a greater risk of disproportionate impact on the right. Whilst the provision of an 'opt-out' clearly contributes to providing this, it seems highly questionable that such an approach is actually very effective. I would argue strongly that any description of opt-out as securing 'implied consent' considerably overstates its practical impact.

It is important that these human rights 'proportionality' requirements are given full weight in any consideration of new legal provision for secondary uses. They could

also usefully be explicitly built into the guidance for applicants for any Section 60 style support.

The secondary use of health and social care information does not seem to have been an issue to come before the Court, but it is possible to argue as to how it would (or should) handle such a case on the basis of these criteria from Art. 8 (2) and in the light of the kinds of protections offered by Article 8 (1). However, there have been two cases which are of particular relevance, namely *Z v Finland (1997)* and *MS v Sweden (1997)*.[15] Several lessons about the potential approach of the ECtHR to Section 60 style provisions for the secondary use of health and social care information can perhaps be drawn from these pivotal cases.

- The Court upholds the principle that article 8 is limited, but considers that the connection between the limitation and an action has to be quite substantial and clear.

- The particular facts in each case were important in the decision taken to disclose confidential information. As secondary uses under Section 60 do not involve consideration of each use or disclosure in the case of each person, there is greater risk of the procedure leading to a violation of someone's rights under the Convention. Without a process that involves judgements in individual cases, whether the interference with the right is proportionate cannot be determined. Such processes might be seen as unjustifiable as they could be argued to *inevitably* lead to interferences with the right to private life in some instances.

- The protection of 'private life' is itself seen as a means of achieving the 'protection of health'. The Court is likely to take a complex view of how the limitation of 'protection of health and moral's' of article 8 (2) applies. It is perhaps likely to construe this limitation very narrowly when it comes to secondary uses. The limitation will be read as being coherent with the right of article 8 (1); it cannot be interpreted as being in *fundamental* conflict with that right. The view of the Court on what the 'protection of health' reasonably requires is in general likely to be significantly narrower than that of most public health professionals.

- It is important that people can see the likely consequences of their actions in advance. Under Section 60 arrangements it is perhaps not sufficiently clear to people what will happen to their information should they provide it to health and personal services.

- The kinds of information handling measures required by data protection law (perhaps especially anonymisation and disposal) are important in ensuring any interference with the right is as minimal as possible.

- A possible broad view of the limitation of 'protection of the economic well being of the country' might provide a justification for the limiting effect of Section 60 measures along with 'the protection of health and morals'.

[15] See Appendix 5.

Summary

The concept of "private life" covers: the physical and psychological integrity of a person; aspects of an individual's physical and social identity; gender identification, name and sexual orientation; personal development, and the right to establish and develop relationships with other human beings and the outside world. The ECtHR also considers that the notion of personal autonomy is an important principle underlying the interpretation of the guarantees of Article 8 of the ECHR. Elements of 'private life', namely moral and mental integrity, clearly suggest that article 8 of the ECHR can be engaged even where service user information has been anonymised.

The European Court of Human Rights might take an interpretative approach which effectively sees the narrower range of limitations of the Biomedicine Convention as being those which are most appropriately limiting on the right to private life in the use of health and social care information.

As the protection of the privacy of health and social care information lies at the heart of the right to private life, any Section 60 style measure would have to pass a strong test of its proportionality. Any use would have to impact to the minimum possible extent on privacy. There would have to be close and effective scrutiny of the measure. There would have to be a means for individuals to be heard.

There does not appear to have been a case at the ECtHR on the secondary use of health and social care information, but other relevant cases suggest that current practice may fall well short of what the Court would expect in terms of respect for private life.

6. Implications for a way forward for Northern Ireland?

There are a range of issues of particular importance for Northern Ireland in considering the introduction of an equivalent to Section 60 of the Health and Social Care Act 2001. Gaining the consent of service users to the use of their personal information for secondary purposes and anonymising that information where possible are key means of both meeting legal requirements and building the trust of service users in the health and social care system.

The importance of consent and anonymisation are confirmed by the 'Key Findings' of a recent consultation conducted for the Medical Research Council[16]:

> The qualitative research shows that there is low awareness and understanding of medical research among the general public. Once the concept of medical research is understood, however, some members of the public feel happier, in principle, for their information to be used for those purposes. The two key pillars of anonymity and consent feature highly in the debate over what information should be available, to whom, and in what circumstances. These two themes are central to building trust.
>
> If the public feels in control of their information and its potential uses, then they are likely to be more inclined to allow their personal health information to be used for medical research purposes.
>
> The most common reason for being unlikely or certain not to allow personal health information to be used for medical research purposes is *concern over privacy* (28%).
>
> Results indicate that a majority of the general public feels that *consent should always be sought*. When given a variety of scenarios in which consent might not be essential, no more than a third of the public agrees with them.

The results of this MRC consultation exercise highlight the need for openness and transparency in the handling of service user information and for the active involvement of both service users and the broader public in the design and regulation of systems for the secondary use of information.[17]

---

[16] Medical Research Council, *The Use of Personal Health Information in Medical Research: General Public Consultation Final Report*, (June 2007).

[17] It is important to note two limitations on the results of the MRC consultation exercise. First, it looked specifically at medical research, which is a considerably narrower range of uses than is covered by secondary purposes. Secondly, whilst indications of public opinion are useful in terms of building the trust of service users (which is itself an essential component of the provision of health and social care services), public opinion often conflicts with legal requirements. Rather than the public opinion measured in this way being seen as sufficient to validate practice, service users need to be better informed about the current legal requirements surrounding the protection, use and disclosure of personal information.

Consent

Gaining the consent of service users to the secondary use of their personal information is an important means of respecting their rights and of building their trust in health and social care services. It forms an important part of the common law, data protection law, human rights law and of ethical standards (including as they are defined by statutory regulators). Whilst not appropriate in all circumstances (such as where the public interest requires an overriding statute), the consent of service users should be the normal basis on which the secondary use of their information proceeds.

Having the consent of a service user is sometimes understood as removing the use of information from any further obligation toward the service user. However, from a human rights perspective, it is properly understood as means of ensuring respect for the rights of service users rather than as a way of 'detaching' information from rights-holders.

'Personal autonomy' and the right to self-determination' have been recognised by the ECtHR as important principles underlying the rights protected by the Convention. Respect for autonomy through measures which require gaining consent go a long way to ensuring that any interference with the right to private life is proportionate. However, just as one cannot consent to be murdered in UK criminal law, so one cannot consent to have one's right to private life violated in human rights law. That the right to privacy was voluntary waived is a factor that the courts would take into account, but it is not determining on its own. There are other bases for processing under the DAP98 than consent, so it is not required to meet data protection standards. Having the explicit consent of a service user to a specific use or disclosure guarantees that one can so use or disclose the information in keeping with the DAP98 and common law, but it might still be an unjustified interference with that service user's private life.

The kind of 'opt-out' provided within PIAG procedures clearly does not meet the common law requirement for (implied) consent. If it did, then there would be no need for Section 60 support in conjunction with the opt-out. In any Section 60 type arrangements it should be clear to service users that in opting-out they are not exercising a legal right in that their opt-out is not legally binding, but are in fact dependent upon a public body to make the decision.

The PIAG conditions around moving toward consent and using 'opt-out' in many cases would be useful to help to protect the rights of service users and could be applied in a Northern Ireland context. It is important though that such conditions for support are understood as limited means of ensuring rights, rather than as a waiver of rights.

Under Section 75 of the Northern Ireland Act 1998, public authorities are required 'to have due regard to the need to promote equality of opportunity' between people who belong to any of nine 'equality categories'. These groups are: 'persons of different religious belief, political opinion, racial group, age, marital status or sexual orientation; between men and women generally; between persons with a disability and persons without; and between persons with dependants and persons without'. A policy which relies on 'opt out' from personal information being used or disclosed for

secondary purposes may well have an 'adverse impact' on individuals from certain of the statutory equality categories. It is difficult to imagine that an 'opt-out' policy would in practice provide the same level of protection for the rights of children or people with a disability as for others. Further consideration may need to be given to the differential impact of 'opt-out' policies with respect to different groups in order to ensure that any Section 60 measure was compliant with Northern Ireland equality law.

Anonymisation

The anonymisation of information for secondary uses is also an important means of respecting the rights and of building the trust of service users in health and social care services. It forms an important part of data protection law, human rights law and occasionally of ethical standards (including as they are defined by statutory regulators). Anonymisation is not appropriate in all circumstances as it could make achieving the goals of some secondary uses impossible. However, ordinarily the anonymisation of information from service users should be the normal basis on which the secondary use of their information proceeds.

Anonymised information is sometimes understood as having been removed from *any* legal or moral connection with the service user and hence from any further obligation toward the service user. However, from a human rights perspective, it is properly understood as means of ensuring respect for the rights of service users rather than as a way of 'detaching' information from rights-holders. The 'wholly detaching' view of anonymisation seems to have arisen for two main reasons.

First, anonymised information does not fall under the DPA98 and that Act is often given inappropriate determining weight in considerations about information use and disclosure. Whilst this is correct about the DPA98, as this Report has stressed there can be other legal obligations towards service users and these might preclude the use of anonymised information. It is also important to note that anonymising is clearly a form of data processing and thus the anonymising of service user information itself stands in need of a basis within the terms of the DPA98.

Second, the judgement in the Source Informatics case[18] suggests that there can be no right to privacy in anonymised information and that such information cannot come under an obligation of confidence. This judgement has been comprehensively criticised elsewhere[19] and it is unsafe to rely on for the planning of legislative proposals for the longer term. This judgement makes use of a narrow conception of privacy which is incompatible with the ECHR and HRA98. It is clear that the aspects of the right to private life which are concerned with 'mental integrity' and 'moral integrity' could be engaged even when information has been anonymised.

Given the above, it is important that any equivalent to Section 60 for Northern Ireland should promote the use of anonymisation as a means of protecting the rights of

[18] (2000) 1 All ER 786.
[19] See Beyleveld, Deryck & Elise Histed, 'Betrayal of Confidence in the Court of Appeal', *Medical Law International* 4 (2000): 277-311.

service users, but also recognise the need to justify uses of anonymised information as potential interferences with the rights of service users to private life.

PIAG-style Committee

Good process in decision-making will require a PIAG-style committee to make judgements about particular health and social care uses of service user information.

Those who have an interest in using the information should not be the ones who decide when it is appropriate to use it. It is important that any such committee has appropriate lay representation and that its decisions, policies and guidance are fully human rights compliant and also make explicit consideration of both human rights standards and Northern Ireland equality law conditions for legal support in using confidential information.

Insofar as it had the power to override the common law, approval by the independent committee for any secondary use of service user information should be compulsory rather than optional. That is, no decisions about the existence of an overriding public interest in a secondary use should be made by those with a private interest in the use.

In addition to its role in providing legal support, such a committee should also be able to give binding guidance on good practice. This can be a requirement of the DHSSPS – that any proposed secondary use of service user information is approved by the committee, even where it is planned to take place on the basis of service user consent. Such approval would be in addition to any provision of a Section 60 get out of common law requirements, but significantly strengthens the extent of protection for service user information.

Working with the common law?

The substantive implications of anything other than a short term measure to get health and social care out of their common law obligations on certain conditions are difficult to determine. Section 60 was introduced in a relative hurry and there is not a body of work presenting sound evidence about its effects overall, both in terms of how the laws relating to health information interact and in terms of the trust of patients.

The common law remains a key part of the protection of the people's rights and when privacy cases such as Campbell v MGN[20] demonstrate that the courts are dependent upon it to give effect to the HRA98 right to private life in certain respects.

Concerns about the full compatibility of Section 60 with human rights standards have been expressed above and similar concerns were also put forward by the Northern Ireland Human Rights Commission in response to the Consultation. (See Appendix 3) Consideration should therefore be given to an entirely different approach which builds on the common law as it stands rather than tampering with it. It could be argued that there is no need for a general undermining of the protection provided by the common law, but rather statutory empowerment is needed for specific secondary

[20] [2004] UKHL 22

A general principle governing secondary uses of confidential service user information should be that the overriding of the common law obligation of confidentiality is a matter for legislators, not for regulators. An approach which revises and consolidates the law in the directions of gaining the consent of service users and maximising anonymisation is perhaps the safest way forward. This is in terms both of protecting and promoting the human, legal and moral rights of service users and securing the uses necessary for the provision and development of modern health and social care in an effective and efficient manner.