

The Data Protection Acts 1988 and 2003

Some implications for public health
and medical research



Asim A. Sheikh
Barrister-at-Law

**The Data Protection
Acts 1988 and 2003:
Some Implications for Public
Health and Medical Research**

**Asim A. Sheikh
Barrister-at-Law**

and

**Lecturer in Legal Medicine
Forensic and Legal Medicine
UCD School of Medicine and Medical Sciences**

July 2008

Published by:
Health Research Board
73 Lower Baggot Street
Dublin 2
Ireland

t +353 1 234 5000
f +353 1 661 2335
e hrb@hrb.ie
w www.hrb.ie

@ Copyright 2008 Health Research Board

Foreword

This discussion document examines some of the legal and practice ramifications of the Data Protection Acts 1988 and 2003 for public health and medical research.

The paper was commissioned by the Health Research Board (HRB) subsequent to the expression of general concerns in relation to how the Data Protection Acts would apply to public health and medical research. Many have expressed the concern that a zealously over-regulated and bureaucratic regime would hamper medical research for the wrong reasons. These concerns have been expressed by a number of people in various jurisdictions. Running in a parallel to these particular concerns has been the law, which has developed a rich corpus of reasoning aimed at ensuring that individual autonomy is protected from violation except where an overriding 'public interest' exception requires it. It is only very recently that this parallel is merging and that the call for recognition, by those involved in research and policy makers, of a 'public interest' exception in medical research has begun to be made. The well-considered merging of the ideas of protection of individuals and proper permissibility in medical research will ensure that medical research will flourish in an atmosphere of trust and thorough but comfortable governance.

Since the commissioning of this paper in 2004, there has been much discussion and work done in relation to attempting to create a reasonable regime of data protection in the field of public health and medical research in this and other jurisdictions. That work has been of great assistance to this document.¹

It is hoped that the conclusions of this document will demonstrate that whilst the Data Protection Acts may bring a degree of inconvenience and bureaucracy to the practice of medical research and public health, that in fact they do not hinder medical research or public health practice, but rather encourage a regime of transparency and the provision of greater information to research participants and patients. This increase in information flow to patients and other individuals, it is hoped, will ultimately ensure that medical research has a solid future.

Comparison with other jurisdictions (as examined in Chapter 4) demonstrates that Ireland does not seek to impose impossible or unworkable restrictions on medical research. There is also an increasing expression from the research communities of the need for public education in relation to matters of public health and medical research. This is so that the population may understand the many public health advantages that involvement in research has brought to

¹ Examples of this work are seen throughout this opinion and are listed in the further reading/ bibliography section at the end of this document.

society. The grounding Data Protection Directive itself recognises the importance of public health. This education should be incorporated into every aspect of healthcare and in any government health initiatives or future reform concerning health data or information so that the public always has readily accessible and easy-to-understand information in relation to what research takes place for the benefit of public health.

This document does not aim to provide answers to every data-protection issue that researchers may have issue with, but rather to highlight the main provisions of concern and make certain suggestions for clarity and improved practice. It may very well be the case that many research protocols will have to be dealt with on a case-by-case basis. However, it is hoped that this document may contribute in some small way, along with other growing work in this area, and that it will foster discussion, debate and promote awareness and that it may assist all those involved in public health and medical research.

Practitioners must also be aware that an integral part of the theory of data-protection practice is its everyday application. Whilst any national measures for record keeping, sharing and quality control will undoubtedly have positive effects on the delivery of better healthcare, seemingly 'minor' issues, which are often taken for granted on an everyday basis, must also be taken into account. Thus, for example, the carriage of patient personal data on a laptop, disc or USB key without password protection may seem inconsequential, but this is not the case. Recent well publicised examples, in this and other jurisdictions, of breaches of data-protection practice demonstrate how serious the ramifications can potentially be for data subjects in terms of their privacy. Security of data is integral to any discussion pertaining to data protection. The rights to privacy and confidentiality and the protection of these long-recognised values are not to be taken lightly. The integration of data protection practice into every part of the healthcare community and its work cannot be emphasised enough. Thus, the call for education is applicable for both patients and healthcare providers.

This document will discuss:

- Chapter 1: The general issues of law that pertain to privacy and confidentiality in relation to medical information.
- Chapter 2: The Data Protection Act in general and its background; the Data Protection Act with application to medical research; an examination of certain case studies to explore the difficulties that the Act poses in its application to certain types of research protocols; a discussion of whether regulation/legislation is required to resolve concerns.
- Chapter 3: Disclosure of records of the dead.
- Chapter 4: An overview and selected comparison with other jurisdictions.

The complexity of this area of law and practice has necessitated detailed discussion. Where detailed legal issues were required to be discussed, these have been done so in the footnotes where possible.

It should be noted that this area of law and practice is in a state of evolution. Where doubt as to practice exists, contact should be made with the Data Protection Commissioner (www.dataprotection.ie) and in cases of doubt or where a fear of breaching confidentiality exists, legal advice should be sought. The importance of documenting carefully decisions relating to disclosure of confidential information and its justification is advised and emphasised here.

The term 'data' is used in relation to the singular and plural in this document.

Acknowledgements

I must firstly express my gratitude to the Health Research Board (HRB) and especially to Dr Teresa Maguire, Dr Maura Hiney and Dr Ruth Barrington (former Chief Executive Officer of the HRB). Whilst this work has taken longer to complete than first envisaged, the advantage has been that many others have also expressed their opinions in this area. The wisdom of those opinions has been very helpful and those opinions are cited widely in this document.

I must also express my appreciation and gratitude to those who have assisted and offered assistance and support: Áine Clancy BL carried out detailed research in relation to the practice in other jurisdictions. This is contained in Chapter 4. To my parents and brother, Haaris Sheikh, for their unfailing encouragement and support as always; to my colleagues and friends inside and outside the Law library and especially to Emily Farrell BL, Leigh Hamilton BL, Bríd Moriarty BL and Leesha O'Driscoll BL for their help and support; at Forensic and Legal Medicine, University College Dublin School of Medicine and Medical Science, to Professor Denis Cusack, Mrs Brid McCormack, Dr Cliona McGovern and Dr Andrew Wilkinson, a word of thanks for their constant support also. A special note of thanks must go to Christine Elise Mani who always offered advice, encouragement and support and who, despite my demanding work load, always remained cheerful, positive and rarely ever complained. I dedicate this effort to her.

Asim A. Sheikh
Barrister-at-Law

Table of Contents

Foreword	1
Acknowledgements	4
Table of Contents	5
1 Health information, confidentiality and privacy	7
1.1 Introduction	7
1.2 Ethical codes and professional guidelines	9
1.3 Law: international statements/treaties	12
1.4 Law: the common law	20
1.5 Law: legislation	27
1.6 Conclusions	32
1.7 Concluding comments	34
2. The Data Protection Acts, 1988 and 2003: some implications for public health and medical research	35
2.1 Introduction	35
2.2 The directive, the Acts and the new obligations	36
2.3 Overview of sections 2, 2A–2D and the exemptions: Main obligations at issue	44
2.4 Types of consent	62
2.5 Conclusions	75
2.6 Concluding comments	77
3 Records, disclosure and the deceased	81
3.1 Introduction	81
3.2 The data-protection issues	81
3.3 Health data for research and the dead: where the Acts do not apply	83
3.4 Conclusions	91
3.5 Concluding comments	92
4 Implementation of the data-protection directive in Europe in relation to medical research	93
4.1 Introduction	93
4.2 Exemptions to the data-protection principles in European legislation	94
4.3 Article 13 and exemptions in relation to medical research	117
4.4 Conclusions	123
4.5 Concluding comments	124
5. Bibliography	125
5.1 Articles, books, guidelines and reports	125
5.2 Cases	128
5.3 Legislation, law, ethical policies, recommendations, opinions	129

1 Health information, confidentiality and privacy

1.1 Introduction

The issues of confidentiality and privacy in healthcare are undoubtedly central in maintaining the healthcare provider/healthcare receiver (patient) relationship. The patient expects that his/her medical information can be given in confidence to a healthcare provider and maintained securely and confidentially by the healthcare provider without any unauthorised third party being allowed access to this information. The doctor–patient relationship can only operate and succeed in such circumstances of trust that result in a full and frank exchange of medical information between the parties. Thus, a patient normally provides his/her medical information to the doctor, who in turn utilises, records and maintains this information for the purposes of treatment and diagnosis. This is the classical mechanism of the doctor–patient data flow and is the primary purpose/use of data in such a setting. In a clinical setting, and in the absence of an indication otherwise, a patient will be entitled to expect that the information he/she gives to a healthcare provider will be used only for his/her treatment and diagnosis. A patient does not have a reasonable expectation that his/her information will be used for any other purpose without being informed of those other purposes.

However, there are many other types of data flow, many of which the public may be unaware of. In this respect, the informational deficit will in most circumstances be presumed to be that of the patient's. Thus, for example, personal data may be used in a healthcare setting for audit, clinical risk management and quality assurance which may well be relation to administration and the overall quality of healthcare that a patient receives. These are secondary purposes/uses as they may be ancillary to the primary purpose.

Within any healthcare system, the research and/or public health community may also wish to use patient data for the purposes, amongst others, of disease investigation, surveillance and intervention, epidemiological studies and longitudinal studies. The realm of 'human research' may be very wide as described by the Australian *National Statement on Ethical Conduct in Human Research*:

Human research is conducted with or about people, or their data or tissue. Human participation in research is therefore to be understood broadly, to include the involvement of human beings through:

- taking part in surveys, interviews or focus groups
- undergoing psychological, physiological or medical testing or treatment
- being observed by researchers
- researchers having access to their personal documents or other materials
- the collection and use of their body organs, tissues or fluids (e.g. skin, blood, urine,

saliva, hair, bones, tumour and other biopsy specimens) or their exhaled breath

- access to their information (in individually identifiable, re-identifiable or non-identifiable form) as part of an existing published or unpublished source or database...²

There is acceptance of the need for such research and for it to be conducted within a balanced framework of protecting the rights of participants and not unduly nor improperly hindering research that is of clear importance to public health.³ Thus, the Medical Research Council in their document, *Personal Information in Medical Research*,⁴ observes that:

Research based on medical records has led to many important advances in medical knowledge and public health, e.g. recognition of vCJD; improvements in the organisation and quality of cancer treatment; improving preventive care for groups at risk of heart attacks and other serious illness. In each case a careful ethical decision is needed, balancing the value of the study and the feasibility of consent against the infringement of confidentiality involved, before deciding whether the research is acceptable.

That medical information is private and confidential is not in contention, and the general concept of medical data/information and its confidentiality and privacy is a long-accepted principle – from the Hippocratic tradition⁵ to modern ethical codes and at common law, certainly in relation to medical information in a clinical setting.

This chapter examines some common themes that have arisen from ethical codes, law and other studies. The chapter will enforce the importance of the norms of privacy and confidentiality, which will subsequently lead to the discussion of how these norms play into the data-protection legislation in relation to public health and medical research.

² Developed jointly by National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, 2007, at 8.

³ The Irish Council for Bioethics (ICB) in their document *Human Biological Material: Recommendations for Collection, Use and Storage in Research* 2005, at ii, state, albeit in relation to biological material and research that 'The collection of human biological samples and their importance and value to medical research is neither a matter of contention nor debate: for medical research to progress and flourish, medical researchers need to have and to study human biological samples. Much progress in healthcare has been achieved by such research.'

⁴ *MRC Executive Summary* (Medical Research Council, UK, 2000–2006) at 1.

⁵ The Hippocratic Oath states 'All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not be spread abroad, I will keep secret and will never reveal.'

1.2 Ethical codes and professional guidelines

The *International Code of Medical Ethics*⁶ states that:

A physician shall respect a patient's right to confidentiality. It is ethical to disclose confidential information when the patient consents to it or when there is a real and imminent threat of harm to the patient or to others and this threat can be only removed by a breach of confidentiality.

The *Declaration of Helsinki*,⁷ which deals specifically with medical research, states at Article 1 that:

The World Medical Association has developed the Declaration of Helsinki as a statement of ethical principles to provide guidance to physicians and other participants in medical research involving human subjects. Medical research involving human subjects includes research on identifiable human material or identifiable data.

Article 10 states that:

It is the duty of the physician in medical research to protect the life, health, privacy, and dignity of the human subject.

Article 21 goes on to state that:

The right of research subjects to safeguard their integrity must always be respected. Every precaution should be taken to respect the privacy of the subject, the confidentiality of the patient's information...

The Council for International Organizations of Medical Sciences (CIOMS), in its publication, *International Ethical Guidelines for Biomedical Research Involving Human Subjects*,⁸ makes an important observation and statement in relation to the general obligation of doctor–patient confidentiality, but also makes a distinction between the normal clinical setting and the setting of an epidemiological study. It guidelines states:

Patients have the right to expect that their physicians and other health-care professionals will hold all information about them in strict confidence and disclose it only to those who need, or have a legal right to, the information, such as other attending physicians, nurses, or other health-care workers who perform tasks related to the diagnosis and treatment of patients. A treating physician should not disclose any identifying information about patients to an investigator unless each patient has given

⁶ World Medical Association, revised 2006.

⁷ World Medical Association, revised 2000.

⁸ CIOMS, 2002 at 76.

consent to such disclosure and unless an ethical review committee has approved such disclosure.

Physicians and other health-care professionals record the details of their observations and interventions in medical and other records. Epidemiological studies often make use of such records. For such studies it is usually impracticable to obtain the informed consent of each identifiable patient; an ethical review committee may waive the requirement for informed consent when this is consistent with the requirements of applicable law and provided that there are secure safeguards of confidentiality... In institutions in which records may be used for research purposes without the informed consent of patients, it is advisable to notify patients generally of such practices; notification is usually by means of a statement in patient-information brochures. For research limited to patients' medical records, access must be approved or cleared by an ethical review committee and must be supervised by a person who is fully aware of the confidentiality requirements.

Here, it can be seen that where an absence of consent is claimed to be justified, such justification requires safeguards of confidentiality.

In its detailed discussion on human research the Australian report *National Statement on Ethical Conduct in Human Research*⁹ discusses from the outset four 'values and principles of ethical conduct' in human research, which it lists as follows: (i) research merit and integrity; (ii) justice; (iii) beneficence; and (iv) respect. As part of 'respect', the report states that:

Researchers and their institutions should respect the privacy, confidentiality and cultural sensitivities of the participants and, where relevant, of their communities. Any specific agreements made with the participants or the community should be fulfilled.

The Australian Code for the Responsible Conduct of Research,¹⁰ in relation to maintaining confidentiality of research data and primary materials, states that:

Researchers given access to confidential information must maintain that confidentiality. Primary materials and confidential research data must be kept in secure storage. Confidential information must only be used in ways agreed with those who provided it. Particular care must be exercised when confidential data are made available for discussion.

⁹ Developed jointly by National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, 2007.

¹⁰ Jointly issued by the National Health and Medical Research Council, the Australian Research Council and Universities Australia, 2007.

In relation to Irish guidelines, the Irish Medical Council's *Guide to Ethical Conduct and Behaviour*¹¹ states that:

Confidentiality is a time-honoured principle of medical ethics. It extends after death and is fundamental to the doctor/patient relationship. While the concern of relatives and close friends is understandable, the doctor must not disclose information to any person without the consent of the patient...

In their document *Operational Procedures for Research Ethics Committees: Guidance*¹² the Irish Council for Bioethics comment on the significance of privacy and confidentiality, stating that:

Privacy and confidentiality are an integral part of the protection and promotion of human dignity and help to protect and maintain a person's mental or psychological well-being. The need for research should be weighed against infringements of privacy and steps must be taken to ensure that individuals are protected from any harm that might be caused as the result of access to their personal information.

The European Standards on Confidentiality and Privacy in Healthcare¹³ are a comprehensive set of principles, which are described as:

...primarily ethical standards. They also consider European legal obligations upon healthcare professionals and the general legal context within which professional decisions about the protection, use and disclosure of confidential information take place. The legal context of this ethical guidance includes shared legal principles and law enforceable within Europe (such as the EU Data Protection Directive and the European Convention on Human Rights). Such laws do not exhaust the obligations on healthcare professionals to respect and protect patient confidentiality and privacy. Healthcare professionals may also need to exercise professional judgment. These Standards provide ethical guidance to all healthcare professionals in the making of such judgments.¹⁴

They discuss the ethical and legal background to the concept of confidentiality within a European setting and state that:

All patients have the right to privacy and the reasonable expectation that the

¹¹ The Medical Council, Sixth Edition, 2004.

¹² Irish Council for Bioethics, 2004, see further at: www.bioethics.ie

¹³ The preface to the standards describes this project as follows: 'These European Standards on Confidentiality and Privacy in Healthcare were developed through the work of the EuroSOCAP Project (QRLT-2002-00771). EuroSOCAP is a European Commission funded project (2003-2006) established to confront and address the challenges and tensions created within the healthcare sector between the information or knowledge-based society and the fundamental legal and ethical requirements of privacy and confidentiality of healthcare information.'

¹⁴ *ibid.*, at 3.

confidentiality of their personal information will be rigorously maintained by all healthcare professionals. Each patient's right to privacy and the professional's duty of confidentiality apply regardless of the form (for example, electronic, photographic, biological) in which the information is held or communicated. Not all healthcare professionals are bound by the same legal obligations of confidence, but all are under the same ethical obligations to maintain confidentiality. Particular care is needed on the part of healthcare professionals to ensure that the right to privacy of vulnerable patients is respected and that their duty of confidentiality toward them is fulfilled.¹⁵

1.3 Law: international statements/treaties

There is growing jurisprudence in the area of privacy. A number of laws and international treaties discuss the right to privacy.¹⁶

The ***Universal Declaration of Human Rights, 1948*** at Article 12 states that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The ***European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950*** at Article 8 states that:

(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.

In this regard, Article 8(2) deals with the justified interference with the right to privacy on certain 'public interest' grounds. The European Court of Human Rights in the case of *MS v Sweden*¹⁷ made some important observations in relation to the right to privacy and

¹⁵ *ibid.*, at 4. These standards will be discussed further in this discussion paper.

¹⁶ *The European Standards on Confidentiality and Privacy in Healthcare* (EuroSOCAP), referred to above at fn 13, are an excellent reference to a number of sources of international privacy laws, some of which are discussed here.

¹⁷ Reports 1997–IV 1437, (1999) 28 EHRR 313. This case concerned an individual (MS) who was diagnosed with spondylolisthesis, in 1965, when she was 14. It is a condition affecting the spine which can cause chronic back pain. In 1981, at the age of 30, MS suffered from a fall at work. She was pregnant at the time and was attending a public clinic. She went to the same clinic in relation to her work injury. She suffered from severe pain and was unable to return to work. In 1991 she

confidentiality stating that:

The Court reiterates that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention.¹⁸

The court observed that the disclosure of the records served a different purpose than that for which it was collected and found that there had been an interference with the privacy of MS which was protected by Article 8(1). It stated that:

The Court notes that the medical records in question contained highly personal and sensitive data about the applicant, including information relating to an abortion. Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants... Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office... Having regard to these considerations, the Court finds that the disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life guaranteed by paragraph 1 of Article 8. It remains to be determined whether the interference was justified under paragraph 2 of Article 8.

In examining the application of Article 8(2) to the facts, the court found that there had been justified reasons for the disclosure and thus no overall breach of Article 8:

made a claim for compensation under the Industrial Injury Insurance Act 1976 to the Social Insurance Office. In 1992, the clinic passed on the medical records of MS to this office at their request and which records included details in relation to an abortion which the patient had in the past due to back problems with a previous pregnancy. This was done without consulting MS: however, the relevant Act obliged all parties to supply, seek and receive relevant information. Secrecy applied to the information if disclosure would harm the person. Subsequently, her application for compensation was rejected. She complained, under Article 8 of the Convention, that the submission of her medical records to the Social Insurance Office constituted an unjustified interference with her right to respect for private life. The court, however, found that there had been no overall violation and her case failed.

¹⁸ At paragraph 41.

The Court considers that there were relevant and sufficient reasons for the communication of the applicant's medical records by the clinic to the Office and that the measure was not disproportionate to the legitimate aim pursued. Accordingly, it concludes that there has been no violation of the applicant's right to respect for her private life, as guaranteed by Article 8 of the Convention.

Thus, here, there are important observations from the court: (i) there is an obligation to protect the patient's sense of privacy (to preserve the patient's confidence in the medical profession and of the healthcare system); and (ii) even where confidentiality is maintained (as it was here – although there had been disclosure to a wider circle of public servants) if the secondary purpose of the information is different to that for which it was first collected, then without the patient's consent, this may be an interference with the patient's privacy; (iii) whatever may be the finding in this regard, it will then be examined whether or not the interference was necessary in accordance with Article 8(2) examining the concepts of whether disclosure was for **relevant** and **sufficient reason** and was **proportionate to the legitimate aim pursued**.

The idea of a patient's 'sense of privacy' was seen in the context of medical treatment in Ireland in the case of *In re a Ward of Court*¹⁹ where the question of the lawfulness of withdrawing artificial nutrition and hydration in a patient who was diagnosed as being in a 'near-PVS' condition arose.

Justice Denham, in the Supreme Court stated that:

Part of the right to privacy is the giving or refusing of consent to medical treatment. Merely because medical treatment becomes necessary to sustain life does not mean that the right to privacy is lost, neither is the right lost by a person becoming insentient. Nor is the right lost if a person becomes insentient and needs medical treatment to sustain life and is cared for by people who can and wish to continue taking care of the person. Simply it means that the right may be exercised by a different process. The individual retains their personal rights.

The right to privacy is not absolute. It has to be balanced against the State's duty to protect and vindicate life. However, '...the individual's right to privacy grows as the degree of bodily invasion increases'. See *In re Quinlan* ...

An unspecified right under the Constitution to all persons as human persons is dignity — to be treated with dignity. Such right is not lost by illness or accident. As long as a person is alive they have this right. Thus, the ward in this case has a right to dignity. Decision-making in relation to medical treatment is an aspect of the right to privacy;

¹⁹ [1996] 2 IR 79.

however, a component in the decision may relate to personal dignity. Is the ward, as described by Brennan J. in his dissenting judgment in *Cruzan v. Director, Missouri Department of Health*... 'a passive prisoner of medical technology?' If that be so, is it in keeping with her right as a human person to dignity? Just as 'the individual's right to privacy grows as the degree of bodily invasion increases': *In re Quinlan*... so too the dignity of a person is progressively diminished by increasingly invasive medicine.²⁰

Denham's juxtaposition of the rights to privacy and dignity in the above context were both balanced in comparison to the bodily invasion that the ward had to endure. Thus, as bodily invasion increased, the dignity of the individual decreased and their right to privacy increased. It might be suggested here that an individual's sense of privacy and dignity will be protected where an external threat occurs which may cause an individual to potentially suffer from a loss of control of their autonomy. In the context of the *Ward* case, the degree of bodily invasion was part of that loss of control. In these circumstances, the law will seek to protect the privacy of the individual, perhaps to seek to minimise the loss of control that an individual will suffer over their autonomy.

Messrs McMahon and Binchy describe Denham J.'s analysis as a radical discussion of privacy and state that 'What emerges is a strongly individualist norm in which choices affecting oneself must be respected by others even where this has damaging or even lethal, consequences.'²¹ Clearly, this 'individualist norm', having balanced and weighed competing interests, is the law's effort in this case to protect a patient's bodily/personal autonomy.

This emphasis on patient autonomy is also seen in the clinical context of the disclosure of risks to patients. This will encourage candour within the doctor-patient relationship. The High Court in Ireland, in the case of *Geoghegan v. Harris*,²² promulgated the 'reasonable-patient test' as being the correct law in relation to the disclosure of risks to patients. The court stated that doctors have a duty to disclose all material risks to patients. This was recently confirmed by the Supreme Court in the case of *Fitzpatrick v. Eye and Ear Hospital*.²³ An example of this rationale

²⁰ at 163.

²¹ McMahon B and Binchy W. *Law of Torts* (3rd edn 2000) at 1022.

²² *Geoghegan v. Harris* [2000] 3 IR 536.

²³ [2007] IESC 51, (Unrep., SC, Kearns, Macken, Finnegan JJ., 17 November, 2007). In that case, in the context of elective surgery, the court commented in relation to the timing of consent, Kearns J., stating that 'There are obvious reasons why, in the context of elective surgery, a warning given only shortly before an operation is undesirable. A patient may be stressed, medicated or in pain in this period and may be less likely for one or more of these reasons to make a calm and reasoned decision in such circumstances. In the instant case, the plaintiff had his eyesight fully tested and evaluated four months before his operation and the options for surgical intervention were plain from the orthoptist's report from that time. The plaintiff was seen on three occasions prior to his operation. The risks associated with squint surgery could have easily been explained to the plaintiff at any of these meetings, or certainly well in advance of the time when they were explained – a mere 30 minutes before his operation. While I have noted the views of a number of the experts to the effect that this practice of warning day patients on the day of their operation had its

was also recently seen in the United Kingdom in the House of Lords decision in *Chester v. Afshar*.²⁴ These cases demonstrate a move towards a more open medical relationship. Within the medical research community in Ireland, the need to respect the autonomy of patients and research participants by providing information to such parties has also been observed.²⁵

Interestingly though, individual rights to bodily integrity may be compromised on the premise of the 'common good', where that interference is minimal, for example, in the context of the mandatory fluoridation of water where such action was deemed to be constitutional. Thus, Dálaigh C.J. in the Supreme Court in the case of *Ryan v. Attorney General* stated that:

The State is organised for the common welfare of all its citizens and is a society arising from man's nature. Apart from particular expressed limitations contained in the Constitution, the Oireachtas may not enact legislation depriving citizens of their essential rights as human persons or as members of the family. The State has the duty of protecting the citizens from dangers to health in a manner not incompatible or inconsistent with the rights of those citizens as human persons.

Dental caries is no new thing. It has adversely affected generation after generation and will continue to do so if measures are not taken. This constitutes the type of danger from which the State has not merely the right but the duty to protect its citizens. To deal with the problem the Oireachtas has chosen a method, namely, the fluoridation of the public water supply. The plaintiff has failed to refute the evidence that this is not only the most effective method but is indeed the only effective method. The method undoubtedly does result in a minimal interference with the constitution of the body, but such interference is not one which in any way impairs the functions of the body or, to any extent discernible by the ordinary person, its appearance.²⁶

Should the same sense of privacy and the individualistic norm as observed in the *Ward* case, as seen above, be persuasive and respected in order to protect, what Case²⁷ describes as,

advantages, it seems to me that the disadvantages were far greater, including the possibility of an embittered patient later asserting that he was too stressed or in too much pain to understand what was said or to make a free decision and that he was thus effectively deprived of any choice'. As shall be seen in Chapter 2, the issue of the circumstances in which a consent is taken become important in terms of the provision of information to a patient.

²⁴ [2005] (HL) 1 AC 134.

²⁵ See further: Irish Council for Bioethics. *Human Biological Material: Recommendations for Collection, Use and Storage in Research* (Irish Council for Bioethics, 2005). Sheikh AA. *Genetic Research and Human Biological Samples: The Legal and Ethical Considerations* (Health Research Board, 2002) at www.hrb.ie. The Irish College of General Practitioners. *Managing and Protecting the Privacy and Personal Health Information in Irish General Practice: An Information Guide to the Data Protection Acts for General Practitioners* (The Irish College of General Practitioners and the National General Practice Information Technology Group, 2003).

²⁶ IR [1965] 294 at 348–9.

²⁷ Case P. 'The rise and fall of informational autonomy in medical law' [2003] 11, 2 *Med. L. Rev.* 208. It has been stated by Phillipson that, 'It is clear that control over personal information, especially

'informational autonomy'? If so, what are the competing interests to be balanced and weighed? This is a matter, central to the theme of this document, which will be discussed later in this Chapter.

Comment 1

In Ireland, privacy is protected as a Constitutional and human right. A healthcare receiver's privacy/sense of privacy must be respected and is integral to the healthcare provider–receiver relationship. It provides the basis for full and frank exchange of information and creates an atmosphere of trust.

Comment 2

The right to privacy imbues a healthcare receiver/patient/research participant with control over their personal autonomy. The compromise of bodily integrity may be permissible, where it is minimal to the individual, but in the common good.

Comment 3

It may be suggested that personal autonomy can be 'bodily autonomy' and 'informational autonomy' and that the according duties of healthcare professionals may differ in relation to either.

It is worth mentioning, and has been seen, that the concepts of 'confidentiality' and 'privacy' are different. Several commentators have pointed this out. The concept of privacy seems to pertain to the control which a person has over themselves. Confidentiality is the duty to respect that information (which has the quality of confidence, e.g. a medical record) which a person entrusts to another on the expectation that it will be kept confidential or which would be regarded to be disproportionate to disclose.²⁸

Lennon notes the distinction and cites from the Canadian Federal Privacy Commissioner who stated that:

People think that they are talking about privacy, when what they are actually talking about is...confidentiality. That I want to emphasize is a mistake. They're entirely

information relating to personal relationships, is essential, not only as an aspect of human dignity and autonomy, but also as a means of ensuring such unimpeded development.' in 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 *Med. L. Rev.* 726 at 732.

²⁸ The concepts were commented on by Lord Nicholls in the case of *Campbell v. MGN Ltd* [2004] 2 AC 457 at 465 when he stated that 'the law imposes a "duty of confidence" whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase "duty of confidence" and the description of the information as "confidential" is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called "confidential". The more natural description today is that such information is private.'

separate issues. Privacy is our right to control information about ourselves-including the collection, use, and disclosure of that information. Confidentiality is your obligation to protect someone else's personal information in your care, to maintain its secrecy and not misuse or wrongfully disclose it...It's privacy that drives the duty of confidentiality...²⁹

Comment 4

The concepts of privacy and confidentiality are distinct but related in the context of medical data. These are both developing areas of law.

It should also be noted that Ireland has now incorporated the European Convention on Human Rights and Fundamental Freedoms, 1950, by virtue of the ***European Convention on Human Rights Act, 2003***.³⁰

In relation to the courts, the Act states at section 2 that:

In interpreting and applying any statutory provision or rule of law, a court shall, in so far as is possible, subject to the rules of law relating to such interpretation and application, do so in a manner compatible with the State's obligations under the Convention provisions.

At section 3 it states that:

Subject to any statutory provision (other than this Act) or rule of law, every organ of the State shall perform its functions in a manner compatible with the State's obligations under the Convention provisions.

Individuals can recover damages for a breach. Section 3(2) states:

A person who has suffered injury, loss or damage as a result of a contravention of *subsection (1)*, may, if no other remedy in damages is available, institute proceedings to recover damages in respect of the contravention in the High Court (or, subject to *subsection (3)*, in the Circuit Court) and the court may award to the person such damages (if any) as it considers appropriate

²⁹ Lennon, P. *Protecting Personal Health Information in Ireland: Law & Practice* (Oak Tree Press, 2005) at 67, citing the Data Protection Commissioner (1998).

³⁰ Lennon notes that, in relation to the incorporation of the Convention in Ireland, the method adopted was 'to avoid, as far as possible, any risk of possible interference with the legislative supremacy of the Oireachtas or the judicial supremacy of the courts and to provide that, subject to the Constitution, statute law and rules of common law should be interpreted in a manner consistent with the State's obligations under the Convention', *ibid.*, at 35.

Comment 5

Irish law now falls to be interpreted in a manner compatible with the obligations of the European Convention of Human Rights and State organs must perform their functions in accordance also with those obligations.

Council of Europe 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, 1997³¹ (also known as the 'Oviedo Convention') states at Article 10:

- (1) Everyone has the right to respect for private life in relation to information about his or her health.
- (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 goes on to state that:

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 ***Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, 2005*** states at Article 25(1) that:

Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life.

The ***Charter of Fundamental Rights of the European Union, 2000*** states:

Article 7: Everyone has the right to respect for his or her private and family life, home and communications.

Article 8: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or

³¹ It should be noted that Ireland, at the time of writing, has neither signed nor ratified this Convention.

her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

The ***Universal Declaration on Bioethics and Human Rights, 2005*** at Article 9 states that:

The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law.

1.4 Law: the common law

In Ireland, the right to privacy is protected as an unenumerated constitutional right,³² the courts stating that:

Though not specifically guaranteed by the Constitution, the right of privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State. It is not an unqualified right. Its exercise may be restricted by the constitutional rights of others, by the requirements of the common good and is subject to the requirements of public order and morality. There are many aspects to the right to privacy...³³

Justice Denham in the case of *In re a Ward of Court*³⁴ observed that:

"The right to privacy is an unenumerated right under the Constitution. The right to privacy was mentioned in *Ryan v. Attorney General* [1965] I.R. 294, and marital privacy was the basis for the decisions in *McGee v. Attorney General* [1974] I.R. 284. In *Norris v. Attorney General* [1984] I.R. 36, the majority refused the plaintiff's claim of privacy but its existence was noted. In two dissenting judgments the right of privacy was expressly recognised. Henchy J. stated at p. 71:—

'...a right of privacy inheres in each citizen by virtue of his human personality, and that such right is constitutionally guaranteed as one of the unspecified personal rights comprehended by Article 40, section 3.'

He described the right of privacy as:

³² There is no recognised tort in relation to a breach of privacy. The Privacy Bill, 1996, however, was drafted with the intention of creating such a tort. Section 2 of the Bill stated that 'A person who, wilfully and without lawful authority, violates the privacy of an individual commits a tort (to be known, and in this Act referred to, as the "tort of violation of privacy")'.

³³ *Kennedy v. Ireland* [1987] IR 1 587 at 592 *per* Hamilton P.

³⁴ at fn 19 at 162.

'...a complex of rights which vary in nature, purpose and range (each necessarily being a facet of the citizen's core of individuality within the constitutional order)... the secret ballot...marital privacy... There are many other aspects of the right of privacy, some yet to be given judicial recognition...'

The law in relation to confidentiality stems primarily from common law³⁵ equitable principles and is guided by ethical and practice guidelines (as seen above).

In looking at the nature of confidential information, Lord Greene MR in *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd* stated that:

If a defendant is proved to have used confidential information, directly or indirectly obtained from a plaintiff, without the consent, express or implied, of the plaintiff, he will be guilty of an infringement of the plaintiff's rights... I think that I shall not be stating the principle wrongly if I say this with regard to the use of confidential information. The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge.³⁶

The Irish courts examined the matter in *House of Spring Gardens v. Point Blank*, where Costello J., in the High Court, approved of this dicta and added that, in relation to confidential information, the court:

...must firstly decide whether there exists from the relationship between the parties an obligation of confidence regarding the information which has been imparted and it must then decide whether the information which was communicated can properly be regarded as confidential information... Once it is established that an obligation in confidence exists and that the information is confidential, then the person to whom it is given has a duty to act in good faith, and this means that he must use the information for the purpose for which it has been imparted, and he cannot use it to the detriment of the informant.³⁷

It cannot be in doubt that the information received by a doctor from a patient is confidential, as has been stated above. Nor is it in doubt that a doctor owes his or her patient a duty of confidentiality. Thus, in *Hunter v. Mann*, Boreham J., stated that:

³⁵ It should be noted that the courts have observed the necessity to recognise Article 8 of the European Convention of Human Rights and the right to privacy in the context of an action for a breach of confidence: 'The time has come to recognise that the values enshrined in Articles 8 and 10 are now part of the cause of action for breach of confidence' *per* Lord Nicholls in the House of Lords, in *Campbell v. MGN Ltd* [2004] 2 AC 457 at 465. See further for an analysis of the issues, Delany H. "Breach of confidence or breach of privacy: the way forward" (2005) 27 *Dublin University Law Journal* 151.

³⁶ (1948) RPC 203 at 211.

³⁷ [1984] IR 611 at 663–4.

...in common with other professional men, for instance a priest and there are of course others, the doctor is under a duty not to disclose [voluntarily], without the consent of his patient, information which he, the doctor, has gained in his professional capacity save...in very exceptional circumstances.³⁸

This is also confirmed by the Supreme Court in *National Irish Bank v. RTE*,³⁹ Lynch J., stating that:

There is no doubt but that there exists a duty and a right of confidentiality...as...exists in...relationships such as for example doctor and patient.... This duty of confidentiality extends to third parties into whose hands confidential information may come and such third parties can be enjoined to prohibit the disclosure of such confidential information. There is a public interest in the maintenance of such confidentiality for the benefit of society at large.

It is interesting to note that Costello J., in *House of Spring Gardens*, observes that the duty of the person receiving the information entails that this person 'must use the information for the purpose for which it has been imparted'. This suggests that if the information is used for any other purpose, then that may be interpreted as not acting in good faith. It was observed above, in relation to the case of *MS v. Sweden*, that secondary use without consent was seen as interference with an individual's privacy. *Initial disclosure of purpose* to a patient/research participant thus becomes, and is an important theme of, this document and issue. In looking at the duties of confidentiality, in *W v. Egdell*,⁴⁰ Bingham LJ., in the Court of Appeal stated that:

The decided cases very clearly establish: (1) that the law recognises an important public interest in maintaining professional duties of confidence; but (2) that the law treats such duties not as absolute but as liable to be overridden where there is held to be a stronger public interest in disclosure. Thus the public interest in the administration of justice may require a clergyman, a banker, a medical man, a journalist or an accountant to breach his professional duty of confidence.

In the Court of Appeal's decision in the case of *R v. Department of Health, ex parte Source*

³⁸ [1974] QB 767 at 772.

³⁹ [1998] 2 IR 465 at 494. It is to be noted here that, apart from the recognised relationships where a relationship of confidentiality clearly exists, the court stated that the obligation extends to third parties into whose hands confidential information may come. This may accord with what Lord Nicholls stated in the House of Lords on the *Campbell* case when he stated at 464 that 'This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship...Now the law imposes a "duty of confidence" whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential.'

⁴⁰ [1990] Ch (CA) 359 at 419.

*Informatics Ltd*⁴¹ Source Ltd (S) wished to collect data on the prescribing habits of GPs. S then planned to sell such data to pharmaceutical companies so that they could more effectively market their products. S therefore asked pharmacists, in return for a small fee, to provide them with certain information from the prescriptions they received, that being: (i) name of GP and (ii) quantity and identity of the drug prescribed. S did not want the name of the patient. The Department of Health issued a policy document stating that the anonymisation of such information would not remove the duty of confidence owed to patients since they would not have consented to such use of data. S sought a judicial review of the policy seeking a declaration that that it was wrong in law and that the disclosure by doctors or pharmacists to a third party of anonymous information did not constitute a breach of confidentiality. The court agreed with S, the defendant/respondent, and the head note describes the court's decision given by Simon Brown LJ., stating that:

In a case involving confidences, the disclosure of information by the confidant would not constitute a breach of confidence provided that the confider's identity was protected. In such a case, the law was concerned only to protect the confider's privacy...⁴²

Simon Brown LJ., went on to state that:

...the confidant is placed under a duty of good faith to the confider and the touchstone by which to judge the scope of his duty and whether or not it has been fulfilled or breached is his own conscience, no more and no less...I referred earlier to [the] plea for respect for 'the patient's autonomy'. At first blush the submission is a beguiling one. My difficulty with it, however, is in understanding how the patient's autonomy is compromised by Source's scheme. If, as I conclude, his only legitimate interest is in the protection of his privacy and if that is safeguarded, I fail to see how his will could be thought thwarted or his personal integrity undermined...the concern of the law here is to protect the confider's personal privacy. That and that alone is the right at issue in this case...in a case involving personal confidences I would hold...that the confidence is not breached where the confider's identity is protected...⁴³

⁴¹ [2000] 1 All ER 786.

⁴² *ibid.*, at 786.

⁴³ *ibid.*, at 796–7. The other issue raised in the case was whether or not the anonymisation of such data was in breach of Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data. This was on the basis that Article 8.1 prohibits such 'processing'. The response to this was that the Directive is not applicable to anonymising data just as it would not be to the use or disclosure of anonymous data since such data is not 'personal data'. The Court of Appeal agreed with this contention. It is arguable that this conclusion may be open to question. Anonymised data is where identifiers are removed. Anonymous data is data where there were never any identifiers. Whilst the latter must fall outside the scope of the Directive, the former cannot as the act of anonymising itself is 'processing' – if done by the data processor. Thus, it is only in the case of anonymous data that the provisions of the Directive would not apply, since they would be unidentifiable and would therefore not come within the ambit of the definition of 'personal data', which is, according to Article 2 of the Directive, 'any information relating to an

The court here could not understand the connection between personal information and how autonomy was compromised once identity was protected. Anonymising the data, it seems, on the basis of the *Source Informatics* decision, will protect privacy. However, this decision did not make the connection in relation to the issue of privacy as being a mechanism of allowing individuals to have control over their data. It is that loss of control which leads to a loss of autonomy as was discussed earlier.

The decision has received mixed reviews from legal academics⁴⁴ and the Irish courts have not yet considered a combination of the issues. When the issues are considered, they will have to be done so taking into account the Constitutional rights to privacy and in accordance with obligations as established by the European Convention on Human Rights.

From the authorities above, in relation to confidential information, it becomes clear that disclosing or further using this information for a purpose other than for which it was given without the consent of the patient would normally be a breach of confidentiality. To justify disclosure without the patient's permission/consent normally requires a 'stronger public interest in disclosure' than in maintaining the confidentiality.

Thus, while the duty to maintain a patient's confidentiality is a heavy one, it is not absolute and

identified or identifiable natural person...an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number...'.
⁴⁴

It is partially welcomed by some who state that 'the Court of Appeal has returned the law to the more orthodox (and we have argued correct) position that breach of confidence does not extend to disclosure of anonymised personal information.' At 1072, Kennedy & Grubb *Medical Law* (3rd edn, 2000). However, others have stated that, 'The decision represents a major challenge to the law of confidence in that it shifts the basis of the duty of confidence from the public interest to that of the fairness of use....the proposition now seems to be that there is no breach of confidence where there is no unfairness to the confider in a possible use of information—and this is so even when that use is unauthorised. Put another way, the decision...indicates that the onus has shifted to the confider who feels that his or her confidence has been abused to show unfairness of use before an action will lie. Moreover, it has removed the public interest requirement from the equation, and this is particularly disturbing as it led the court to ignore the wider and longer term impact of its decision on the generality of public interest in maintaining confidences. Arguably, the effect of *Source Informatics* is to reduce the individual's legal interest in his or her information to no more than that of ensuring that anonymity is maintained. In doing so, other fundamental issues are ignored, including the role of consent in legitimising the uses of information, the concept of reasonable expectations of use and, ultimately, the importance of maintaining a prima facie respect for confidences.' Mason and Laurie in *Mason and McCall Smith's Law and Medical Ethics* (7th edn, 2006) at 280. On the basis of the Irish decision in *House of Spring Gardens*, this latter view may better reflect Irish law as the High Court stated that the receiver of confidential information 'has a duty to act in good faith, and this means that he must use the information for the purpose for which it has been imparted, and he cannot use it to the detriment of the informant.' Kennedy & Grubb, *ibid.*, however, state that 'There is a danger in conceptualising the basis of protecting confidences as an aspect of "privacy". Clearly it is...but it is not the same as "privacy"...as protected under Art 8 of the European Convention. The main danger lies in misunderstanding the essence of a breach of confidence as going beyond unauthorised disclosure of information so as to include other unauthorised or improper *uses* of the information...The law should deal with the misuse of personal of information through the protective scheme of the Data Protection Act 1998.' The Irish courts have yet to consider a decision which involves the combination of the issues of confidentiality, privacy and data protection and, thus, the law remains to be definitively tested. *Source Informatics* is discussed further in Chapter 2.

the question arises as to what are the 'public interest' circumstances where a doctor can breach his/her duty of confidence and disclose information to any third party?

In this regard, Paragraph 16.3 of the Irish Medical Council guidelines state that:

There are four circumstances where exceptions may be justified in the absence of permission from the patient:

- (1) When ordered by a Judge in a Court of Law, or by a Tribunal established by an Act of the Oireachtas.
- (2) When necessary to protect the interests of the patient.
- (3) When necessary to protect the welfare of society.
- (4) When necessary to safeguard the welfare of another individual or patient.⁴⁵

As has been seen, in the normal clinical setting, the release of patient information can be done by obtaining the patient's consent to release. For release without consent/permission, a public interest reason is required (with an examination of whether disclosure was for relevant and sufficient reason and was proportionate to the legitimate aim pursued) in the law of confidentiality and privacy. The common law has dealt with a number of well-known cases dealing with situations where the public interest required disclosure of confidential information: where there was a public interest in revealing details of a dangerous prisoner to the state;⁴⁶ where the authorities should be informed of a dangerous individual who seeks to harm another (**preventing harm to others**);⁴⁷ where a wrongdoing must be exposed (**exposing, preventing or detecting crime**);⁴⁸ where an individual institutes litigation and refuses to

⁴⁵ See fn 11. Paragraph 16.4 states that 'Doctors working in Ireland have a responsibility to ensure compliance of their record systems with current Irish Data Protection and Freedom of Information legislation.' Paragraph 20.2 entitled 'Anonymity' states that 'Research results must always preserve patient anonymity unless permission has been given by the patient to use his or her name.' It should be noted that in relation to the status of these guidelines the courts have recently stated that: 'These ethical guidelines do not have the force of law and offer only such limited protection as derives from the fear on the part of a doctor that he might be found guilty of professional misconduct with all the professional consequences that might follow.' in *M. R. v. T. R., Walsh & Ors* [2006] IEHC 359 per McGovern J.

⁴⁶ Thus, in *W v. Egdel* [1990] Ch (CA) 359, disclosure by a psychiatrist of his assessment of his patient, which he disclosed to the Home Secretary in relation to the danger still posed by a prisoner who was due to go before a parole board, was held to be in the public interest.

⁴⁷ In *Tarasoff v. Regents of the University of California* (1976) 131 Cal Rptr 14 (Cal Sup Ct) an individual had threatened to kill another student making this confession to a university psychologist. He passed the information on to the campus police who interviewed the individual and no further action was taken as it was not deemed a danger. He then proceeded carry out his threat and killed the student. The court, *per* Tobriner J., held that 'We recognise the public interest in supporting effective treatment of mental illness and in protecting the rights of patients to privacy...and the consequent public importance of safeguarding the confidential character of psychotherapeutic communication. Against this interest, however, we must weigh the public interest in safety from violent assault...We conclude that the public policy favoring protection of the confidential character of patient-psychotherapist communications must yield to the extent to which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins.'

⁴⁸ In *National Irish Bank v. RTE* [1998] 2 IR 465 the Supreme Court held that 'there is also a public interest in defeating wrong doing and where the publication of confidential information may be of assistance in defeating wrong doing then the public interest in such publication may outweigh the

disclose their medical information to a defendant (**waiver of privacy by a litigant in proceedings**).⁴⁹ Exceptions to the confidentiality rule will also arise by virtue of statute which will require information to be disclosed on clear public interest grounds such as in the context of infectious diseases, child protection and assessment of eligibility of access to health services (**statutory exceptions**).⁵⁰ Messrs Kennedy and Grubb note that 'On disclosure for research purposes, there is precious little authority.'⁵¹

public interest in the maintenance of confidentiality.'

⁴⁹ In *McGrory v. ESB* [2003] 3 IR 407 Keane CJ., at 414 stated that, 'The plaintiff who sues for damages for personal injuries by implication necessarily waives the right of privacy which he would otherwise enjoy in relation to his medical condition. The law must be in a position to ensure that he does not unfairly and unreasonably impede the defendant in the preparation of his defence by refusing to consent to a medical examination. Similarly, the court must be able to ensure that the defendant has access to any relevant medical records and to obtain from the treating doctors any information they may have relevant to the plaintiff's medical condition, although the plaintiff cannot be required to disclose medical reports in respect of which he is entitled to claim legal professional privilege.' In the context of litigation and discovery, Clarke J., in the matter of *Independent Newspapers v. Murphy* [2006] 3 IR 566 at 572, stated that 'I am satisfied that the court should only order discovery of confidential documents (particularly where the documents involve the confidence of a person or body who is not a party to the proceedings) in circumstances where it becomes clear that the interests of justice in bringing about a fair result of the proceedings require such an order to be made. It is clear that confidential information (which is not privileged) must be revealed if not to reveal same would produce a risk of an unfair result of proceedings. The requirements of the interests of justice would, in those circumstances, undoubtedly outweigh any duty of confidence. There is ample authority for that proposition which now may be taken to be well settled. Where, therefore, it is clear that the materials sought will be relevant, then discovery must be made notwithstanding any confidentiality. However, it seems to me that the balancing of the rights involved also requires the application of the doctrine of proportionality. To that extent, it seems to me to be appropriate to interfere with the right of confidence to the minimum extent necessary consistent with securing that there be no risk of impairment of a fair hearing.'

⁵⁰ For example, (i) in relation to **infectious disease**, section 30(2) of the Health Act, 1947 states that 'A person having the care of another person and knowing that such other person is a probable source of infection with an infectious disease shall, in addition to the precautions specifically provided for by or under this Part of this Act, take every other reasonable precaution to prevent such other person from infecting others with such disease by his presence or conduct or by means of any article with which he has been in contact.' This may require the disclosure of the medical details of the infected patient to any other party. (ii) In relation to **child protection**, the powers of the Health Boards (now the Health Service Executive) in this regard are stated in section 3 of the Child Care Act, 1991 which states at s.3(2)(a) that the duty is to 'co-ordinate information from all relevant sources'. The relevant guidelines which deal with the various issues (*Children First* (1999), Department of Health and Children) state at paragraph 5.2.3 that 'Ethical and statutory codes concerned with confidentiality and data protection provide general guidance. They are not intended to limit or prevent the exchange of information between different professional staff who have a responsibility for ensuring the protection of children. Giving information to others for the protection of a child is not a breach of confidentiality.' (iii) In the context of **road traffic law**, under section 107 (4)(c) of the Road Traffic Act, 1961, healthcare staff may be required to identify a patient (in the context of identifying the driver of a vehicle) if requested by the gardaí. Under section 15 of the Road Traffic Act, 1994, the gardaí can, in a hospital, require a person to (a) permit a designated doctor to take from the person a specimen of his/her blood or (b) at the option of the person, to provide for the designated doctor a specimen of his/her urine. It is an offence for such a person not to comply unless 'where following his admission to or attendance at a hospital, the person comes under the care of a doctor and the doctor refuses on medical grounds to permit the taking or provision of the specimen concerned.' (iv) In the *MS* case as examined previously, disclosure within a circle of public servants of medical data as required by legislation, for the purposes of assessing a compensation application, was held not to be in violation of Article 8 of the ECHR. Also discussed above is the SI 105/1971, the Health Services Regulations, 1971, which allows for access to clinical records without a patient's consent in certain circumstances **for the purposes of ascertaining eligibility to health services** as provided for by the Health Act 1970.

⁵¹ *op. cit.*, fn 44, at 1112 where the authors cite one potential authority where disclosure for research

Comment 6

Medical data should, generally, not be disclosed for purposes other than for which it was initially collected or consented to without the healthcare receiver's consent. This is also recognised by common law.

Comment 7

The healthcare provider–healthcare receiver relationship is one of confidentiality and there is a public interest in maintaining this relationship as one of confidentiality.

Comment 8

The healthcare receiver may consent to disclosure of his/her medical data.

Comment 9

There are exceptions to the confidentiality rule where confidentiality can be overridden, without an individual's consent, for the stronger reason of public interest and where privacy can be lawfully interfered with, allowing disclosure where it is relevant, for sufficient reason, in the interests of justice and if is proportionate to a legitimate aim.

Comment 10

The usual types of public interest exceptions occur (i) for the prevention of harm to others; (ii) for the prevention/detection/prosecution of crime or wrongdoing; (iii) where a litigant loses or waives his/her privacy in litigation; (iv) for purposes where statute requires disclosure.

1.5 Law: legislation

There are some legislative provisions which also require adherence to the principles of confidentiality, as discussed above.

SI 105/1971, the Health Services Regulations, 1971, relate to the manner in which and the extent to which certain medical services under the Health Act, 1970 will be provided by the health boards to eligible individuals. The regulations state at section 5(2) that:

is stated. In the Scottish case of *AB v. CD* (1851) 14 D 177, Lord Fullerton at 179–80, in stating that the doctor–patient relationship carries an obligation of secrecy, the court stated, 'The obligation may not be absolute. It may and must yield to the demands of justice, if disclosure is demanded in a competent Court. It may be modified, perhaps, in the case alluded to in the argument of disclosure being conducive to the ends of science, though even there concealment of individuals is usual.' In the *Source Informatics* case, Simon Brown LJ., at 800–1, alluded to the use of identifiable data in research stating that 'provided, as I understand to be the case, the use of such identifiable data is very strictly controlled, there appears no reason to doubt that this is acceptable – whether because it falls within the public interest defence or, is perhaps the preferable view, because the scope of the duty of confidentiality is circumscribed to accommodate it'.

Any clinical records compiled or any document obtained under these Regulations shall be treated in a confidential manner and, save as provided in sub-article (5) of this article, shall not, without the consent in writing of the patient, be disclosed in such a manner as to make identification of the patient possible.

Subsections 4–7 provide for the inspection of clinical records and to dispense with the consent of the patient when it would not be 'in the common interest' to do so. Thus:

(4) Nothing in this article shall be construed as preventing the inspection by a registered medical practitioner authorised by the chief executive officer of the health board or by the Minister of the clinical records kept in pursuance of these Regulations where the written consent of the patient has been obtained.

(5) Where the Minister certifies in respect of clinical records compiled under these Regulations and held by any particular medical practitioner or in relation to any particular patient that it would not in his opinion be in the interest of the common good to seek the consent referred to in subarticles (2) and (4) of this article a registered medical practitioner authorised by the Minister may inspect such records.

(6) Where a certificate under subarticle (5) of this article has been given in respect of any particular clinical records by the Minister and the medical practitioner holding such records is of opinion that the patient to whom the records relate should be informed of the giving of the certificate such medical practitioner may so inform such patient.

(7) The consent referred to in subarticles (2) and (4) of this article may, in the case of a minor, be given by a parent or guardian and, in the case of a deceased person, may be given by the spouse of such person, or if there is no spouse, by any of the next of kin of such person or by his personal representative.

The Data Protection Acts, 1988 and 2003 (which are discussed in detail in the next chapter) encapsulate the concept of confidentiality and privacy.

The Statistics Act, 1993 allows a general exception to the Data Protection Acts for the purposes of, as stated by section 10 of the Act, 'the collection, compilation, extraction and dissemination for statistical purposes of information relating to economic, social and general activities and conditions in the State.' This can be done by the Central Statistics Office and/or with other public authorities and persons. The Act allows for the collection of information of any type, to be used in a non-identifiable way (unless an individual consents to its use in an identifiable way).

Under the provisions of the Act, by virtue of section 21, every person, before assuming duties as an officer of statistics, is obliged to sign a declaration which states that:

I _____, solemnly declare that I will fully and honestly fulfil my duties

as an officer of statistics in conformity with the requirements of the *Statistics Act, 1993*, and of all orders thereunder, and that I will not, except in the performance of my duties under that Act and such orders, disclose or make known during my service as an officer of statistics or at any time thereafter, any matter which comes to my knowledge relating to any person, family, household or undertaking by reason of my service as an officer of statistics.

The Act at section 24 states that:

- (1) The Director General or an officer of statistics may invite a person or undertaking to-
 - (a) complete a form, questionnaire or other record,
 - (b) answer any questions,
 - (c) provide any information or records,on a voluntary basis and any information so obtained shall be subject to the restrictions on use and prohibition on disclosure of information specified in sections 32, 33, 34 and 35 of this Act.
- (2) Persons and undertakings may provide information and records, or copies thereof, which they may possess to the Director General or officers of statistics on invitation under the provisions of this Act notwithstanding anything contained in the Data Protection Act, 1988.

It must be noted above that the general invitation to a person to provide information or records is on a voluntary basis.

In accordance with section 30, public authorities may be obliged to allow access to medical records which are not publicly available, but only with the agreement of the Minister for Health.

In further protecting information collected, section 32 seems to limit the use of the information collected and states that:

All information furnished by a person, undertaking or public authority under this Act shall be used only for statistical compilation and analysis purposes.

Section 33 of the Act deals with the non-disclosure of identifiable information and states that:

- (1) No information obtained in any way under this Act or the repealed enactments which can be related to an identifiable person or undertaking shall, except with the written consent of that person or undertaking or the personal representative or next-of-kin of a deceased person, be disseminated, shown or communicated to any person or body except as follows—
 - (a) for the purposes of a prosecution for an offence under this Act;
 - (b) to officers of statistics in the course of their duties under this Act;

(c) for the purposes of recording such information solely for the use of the Office in such form and manner as is provided for by a contract in writing made by the Director General which protects its confidentiality to his satisfaction.

(2) The Office may, for statistical purposes only, assign codes derived from information collected under this Act classifying undertakings listed in the administrative systems of other public authorities by economic activity and size (persons engaged) categories.

(3) The Taoiseach may by order prescribe such further prohibitions on the disclosure of identifiable records or information obtained under this Act or the repealed enactments for such periods as may be prescribed.

(4) Nothing in this Act shall be construed to require any person or undertaking to provide information in relation to a matter on which information was sought in circumstances that would entitle the person or undertaking to decline to give the information in a civil proceeding in any court or on grounds of privilege.

In relation to passing information on to others, section 34 of the Act states that:

The Office may provide, for statistical purposes only, information obtained in any way under this Act or the repealed enactments, in such form that it cannot be directly or indirectly related to an identifiable person or undertaking, to such persons and subject to such charges, conditions and restrictions as the Director General may determine.

Misuse of information (Section 38) and failure to protect documentation (Section 42) are offences under the Act.

Thus, medical research, the objective of which is statistical only, can be arranged in accordance with this Act. An example of this is the Irish National longitudinal study of children 'Growing up in Ireland' (at: www.growingup.ie).

The Health (Provision of Information) Act, 1997 provides a general exception to the Data Protection Act rules by allowing the National Cancer Registry Board or the Minister for Health or a health board, hospital or other body or agency participating in any cancer screening (including any breast or cervical cancer screening) programme authorised by the Minister for Health, to request from any person information held by or in the possession of that person. That person may provide the information as requested for the purposes of maintaining cancer registries. This matter is discussed later Chapter 2.

The ***Freedom of Information Acts, 1997 and 2003***,⁵² state at section 28(2) that that access to information will be refused to a requester unless the information pertains to that

⁵² The overlaps between the Data Protection and Freedom of Information legislation are discussed by McDonagh in *Freedom of Information Law* (2nd edn 2006), Chapter 20 and by Lennon, *op. cit.*, in Chapter 13.

requester or unless the party about whom the information relates has consented to that information being given to the requester. The information can also be released if it is already in the public domain, if the individual was told that it would be released and if its release is to avoid a serious and imminent danger to the life or health of an individual. The information can also be released if the public interest outweighs the right to privacy of the individual or if the release would benefit the individual.

SI No. 190 of 2004, European Communities (Clinical Trials on Medicinal Products for Human Use) Regulations 2004 govern clinical research. The conditions and principles for the protection of clinical trial subjects are provided for in Schedule 1 and at Part 2 (5) which state that:

The rights of each subject to physical and mental integrity, to privacy and to the protection of the data concerning him or her in accordance with the Data Protection Acts 1988 and 2003, are safeguarded.

In relation to genetic testing, the ***Disability Act, 2005*** at Part IV, section 45 (1) states that:

Nothing in this Part shall be construed as authorising the processing of personal data contrary to the provisions of the Data Protection Acts 1988 and 2003.⁵³

For the purposes of this discussion, in the realm of ever more complex public health issues, data-protection legislation, privacy, confidentiality and health research, the main issue of controversy seems always to be one of competing interests and the balance to be achieved between the protection of confidentiality and the allowing of access to information for health research. These challenges are explained well by the Canadian Institutes of Health Research (CIHR) in its report *Best Practices for Protecting Privacy in Health Research*⁵⁴ which explains these competing interests:

In the area of ethics, one of the key challenges for the health research community is to protect the privacy of individuals and the confidentiality of personal information, at a time of great change in research. For example, technological advances in information

⁵³ Section 42 (3) states that 'A person shall not process genetic data unless all reasonable steps have been taken to provide the data subject with all appropriate information concerning –
(a) the purpose and possible outcomes of the proposed processing, and
(b) any potential implications for the health of the data subject which may become known as a result of the processing.

(4) A person who contravenes *subsection (2) or (3)* shall be guilty of an offence; an offence under this subsection shall be deemed to be an offence to which section 31 of the Data Protection Act 1988 applies. It should be noted that SI No. 687 of 2007 introduced the Data Protection (Processing of Genetic Data) Regulations 2007. The regulations provide for the designation, under section 12A of the Data Protection Acts 1988 and 2003 for the purposes of section 42(2)(a) of the Disability Act 2005, of the processing of genetic data in relation to the employment of a person. Processing that can only take place with the prior approval of the Data Protection Commissioner.

⁵⁴ CIHR, September 2005.

technology and the advance of genetic research are challenging existing standards and mechanisms for privacy protection. Also, the sheer number, diversity and complexity of new privacy laws and policies within and beyond... borders are increasing the practical challenges faced by researchers, particularly for those conducting studies across jurisdictions. And, while there are increasing demands for privacy protection in health research, there is also clear recognition that health research plays a critical role in improving...health... and supporting an evidence-based health care system.

Comment 11

There exists Irish legislation relevant to the healthcare, medical research and public health which requires adherence to the principle of confidentiality and provides for exceptions to the principle in certain circumstances.

1.6 Conclusions

The above discussion demonstrates that legal thinking, texts, and the courts have placed great emphasis on the protection of an individual's autonomy. A loss of control over an individual's personal data, especially sensitive personal data such as medical data, is seen as a loss of autonomy and has led the courts to prevent or minimise such a loss of control. Whilst the common law courts have attempted to carry out this protective function through the equitable doctrine of confidence, the influence of the law of privacy and the jurisprudence of the European Convention of Human Rights is now and will in the future play a dominant part in the courts. In Ireland, this will be allied to the constitutional protection afforded to privacy. The maintenance of confidentiality and respect for privacy are recognised to be in the public interest. To the obligations of confidentiality and respect of an individual's privacy, there also exist exceptions, explored by the courts and specified by statute. These are normally based on some type of public interest override in disclosure. Where a conflict occurs between maintaining confidentiality/privacy and disclosure/freedom of expression, courts, other tribunals and decision makers, will engage in the exercise of balancing and weighing these competing interests and in looking to whether disclosure is relevant, for sufficient reason, in the interests of justice and whether it was proportionate to any legitimate aim pursued. Where new issues arise, the courts will decide the issues on a case-by-case basis.

In medical research – for example, to access a past medical database, or to access past patient records, or to access the records of a deceased patient by a researcher – must patient consent be obtained? The issue of consent and when and in what circumstances it is required seems to cause the most 'tension'. The issue is testing the boundaries of privacy and confidentiality by seeking to allow the flow of data in, what is powerfully argued by some to be, the public good/interest, that is medical research, especially for the requirements of public health.

The issues of law pertaining to data protection, confidentiality and privacy are complex in this regard. The common law courts have not dealt with the provision of a 'medical research public interest' exception to the confidentiality or privacy protections. It has been stated that:

Disclosure of confidential information to third parties outside the health services may be justifiable in order to protect overriding interests of third parties or a legally protected public interest. However, every decision to disclose confidential patient information outside the healthcare services violates the patient's right to privacy, and is in breach of the healthcare professional's obligation of confidentiality. The disclosure will only be justified in exceptional circumstances, that is, if the disclosure serves an interest that in the particular circumstances outweighs the patient's right to privacy. Potential outweighing interests could be the protection of the rights and freedoms of others, national security, public safety, the economic wellbeing of the country, the prevention of disorder or crime, or the protection of health or morals (as suggested by Article 8 (2) of the ECHR).

...whether or not disclosure can be justified... depends on balancing the interests that are in conflict in each case. It needs to be borne in mind that every instance of disclosure leads to a certain violation of the patient's right to privacy, while the benefits of disclosure will often be less certain. While a balancing of the patient's right to privacy against other rights and interests is always difficult, it is usually more easily performed where the conflict is with rights of identifiable third parties, than where there is a conflict with a more diffuse public interest such as national security or public health. It is not sufficient that it might be more convenient for the protection of such interests that information is disclosed, but the test is instead one of strict necessity in the specific circumstances of each case.⁵⁵

The complexities and tensions are strongly expressed by the United Kingdom's Academy of Medical Sciences in their detailed consideration of the issues in their report *Personal data for public good: using health information in medical research*. The introduction states that:

...evidence submitted to the Academy shows that advances in this field are increasingly inhibited by inappropriate constraints on the use of personal health data. These constraints arise through confusing legislation and professional guidance, bureaucracy of process and an undue emphasis on privacy and autonomy. It is essential that data about the health of individuals are only used for research under conditions of confidentiality that enjoy public support. However, evidence of public attitudes towards the use of health information in research is largely absent, forcing regulatory and advisory bodies to

⁵⁵ EuroSOCAP Guidelines, fn 13 at 21 to which healthcare providers should refer to and take into account.

make assumptions about what the public might find acceptable.

These factors have created a conservative culture of governance, where disproportionate constraints are imposed on research that can compromise its quality and validity. The difficulties of the current situation are a significant disincentive for researchers to undertake work in this field and are detrimental to research aimed at improving public health.⁵⁶

Comment 12

The courts have not, in general or in any detailed way, considered the issue of medical research as a public interest exception to the confidentiality rule.

It is with the above discussion in mind of the theory and practice of confidentiality and privacy on the one hand, and the above described tension on the other hand, that the discussion of the Data Protection Acts 1988 and 2003 and their implications for medical research and public health will take place.

1.7 Concluding comments

Comment 13

The protection of an individual's privacy and confidentiality and the assurances and security measures utilised to ensure this protection will be central to successful data protection practice in healthcare, medical research, public health and any future reform in this area.

⁵⁶ *Personal Data for Public Good: Using Health Information in Medical Research: A Report from the Academy of Medical Sciences* (UK, January 2006) at 3. The academy's aims are stated in the introduction to its report which states that : 'The independent Academy of Medical Sciences promotes advances in medical science and campaigns to ensure these are translated as quickly as possible into benefits for patients. The Academy's Fellows are the United Kingdom's leading medical scientists from academia, hospitals, industry and the public service. The aims of the Academy are to: Give national and international leadership in the medical sciences. Promote the application of research to the practice of medicine and to the advancement of human health and welfare. Promote the aims and ethos of medical sciences, with particular emphasis on excellence in research and training. Enhance public understanding of the medical sciences and their impact on society, assess and advise on issues of medical science of public concern.'

2. The Data Protection Acts 1988 and 2003: some implications for public health and medical research

2.1 Introduction

Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data was transposed into national law and is now the Data Protection (Amendment) Act, 2003. Read together the 1988 Act and the 2003 amendment are now the Data Protection Acts 1988 and 2003 (referred hereinafter as 'the Acts').

In light of the discussion in Chapter 1 in relation to the need for the protection of the rights of individuals and the need not to unduly hamper research, it should be noted that the Directive at Recitals 1 and 2 also invokes a spirit of balance between fundamental rights and freedoms, notably the right to privacy, and economic and social progress and the well-being of individuals:

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals...

It has been said that the Directive is 'a self-vowed attempt to harmonise informational privacy protection throughout Europe...founded on the broader commitment of EC member states to protect individual privacy, most notably as embodied in Article 8 of the European Convention on Human Rights.'⁵⁷

The Directive and the transposing Act, when compared to the Data Protection Act, 1988, provide for new obligations to those processing data. The new issue of primary concern to

⁵⁷ Laurie G. *Genetic Privacy: A Challenge to Medico-legal Norms* (Cambridge University Press, 2002) at 251.

many in the research community is that of the deemed necessity to obtain consent prior to the processing of data (Article 7, Directive 95/46/EC). This has caused much concern especially in relation to 'secondary data' or 'archived data' for the purposes of public health medical research. This will be the main emphasis of this chapter.⁵⁸ This chapter will first look at the Acts and their potential interpretation. It will then examine case studies and problems highlighted in medical and public health research.

2.2 The directive, the Acts and the new obligations

2.2.1 What is personal data? Issues of identifiability

The Acts state that '**personal data**' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

The definition does not cover the dead (this will be discussed in Chapter 3 below). Normally medical data, for example contained in a clinical record, is clearly personal data. The patient will usually be *named* (is identified) and the information in the record will be *about* that individual. That individual will be the *focus* of the record and it will record his/her intimate information. There is clearly a substantial link between the individual and the record and the record will speak for itself.⁵⁹ Being personal data, the obligations as discussed below, will apply.

⁵⁸ For general information about the Acts, see further: the Data Protection Commissioner at www.dataprotection.ie and also Lennon P. *Protecting Personal Health Information in Ireland: Law & Practice* (Oak Tree Press, 2005).

⁵⁹ In *EH v. Information Commissioner* (No. 2) [2002] 3 IR 600 at 604. O'Neill J., in the High Court held, in relation to the words 'relates to personal information' contained in the Freedom of Information Acts, that: 'In my view the test to be applied to determine whether or not a record "relates to" is "whether there is a sufficiently substantial link between the requesters personal information (as defined in the act) and the record in question"...' (at 604). However, he went on to state also that: 'A requester has a right of access to "records". The record will generally speak for itself. Where a doubt or ambiguity exists, as to the connection of the record to the requester, a consideration of factors such as the circumstances in which the record was created, the purpose for which the record was created and whether it was created with the affairs of a particular individual in mind, may *inter alia*, assist in determining "whether there is a sufficiently substantial link between the requester's personal information (as defined in the Act) and the record in question" (*ibid.*). O'Neill J., concluded by stating that: 'As said earlier the record will speak for itself. If the record contains an express reference to the requester, be it however, insubstantial or trivial then clearly it "relates to personal information" about the requester. Here one would have in mind records such as letters which contained no personal information but are about or refer to the requester, such as holding type letters or pro forma or replies. Where the record does not name or has no express reference to the requester a substantial link will be established, if the record relates to something in which the requester has a substantial personal interest, as distinct from something in which he has an interest as a member of the general community or of large scale class of the same.' In looking at the definition of 'personal information' in the UK Data Protection Act, 1998, Auld LJ., in the Court of Appeal in the case of *Durant v. Financial Services Authority* [2003] EWCA Civ 1746 at para. 28 stated that: 'It follows from what I have said that not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions

The issue of the words 'can be identified' or 'identifiable' is worth mentioning as it is relevant to the issue of 'anonymous' data and 'anonymised' data.

According to the Directive, personal data is:

...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, cultural or social identity...

Recital 26 of the Directive states that:

Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine 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; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable...⁶⁰

The Data Protection Working Party makes the distinction between direct and indirect identifiability.⁶¹ In relation to the former:

...the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation. A very common family name will not be sufficient to identify someone – i.e. to single someone out – from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as 'the man wearing a black suit' may

or matters in which he may have been involved to a greater or lesser degree. It seems to me that there are two notions that may be of assistance. The **first** is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The **second** is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity' (writer's emphasis). The Data Protection Working Party (see fn 62 at 10–11) state that 'it could be pointed out that, in order to consider that the data 'relate' to an individual, a '**content**' element OR a '**purpose**' element OR a '**result**' element should be present.... These three elements (content, purpose, result) must be considered as alternative conditions, and not as cumulative ones.'

⁶⁰ Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data states that 'the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as anonymous; the expression "medical data" refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data'.

⁶¹ Opinion 4/2007 on the Concept of Personal Data 20/6/07 at 12–13.

identify someone out of the passers-by standing at a traffic light. So, the question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case. Concerning 'directly' identified or identifiable persons, the **name** of the person is indeed the most common identifier, and, in practice, the notion of 'identified person' implies most often a reference to the person's name.

In relation to the latter, the Working Party states:

As regards 'indirectly' identified or identifiable persons, this category typically relates to the phenomenon of 'unique combinations', whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be 'identifiable' because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.

The Working Party then discusses pseudonymised data (such as key-coded data) and states that such data can be indirectly identifiable, whereas anonymous data is where an individual cannot be identified. This issue is of some importance as unidentifiable data is outside the scope of the Act. Thus, if a data controller/processor (e.g. a researcher) were to collect or receive anonymous data, that would fall outside the scope of the Acts as it is not identifiable data and anything the researcher does with that data (i.e. process it) will fall outside the scope of the Acts.

However, if the data was obtained as identifiable data by the researcher and was then anonymised by the researcher, then the act of obtaining and anonymisation by the researcher, it could be argued, is 'processing'⁶², and thus the Acts would apply to this data. That being so, the data subject would have to be told of the intention to anonymise.⁶³ Opinions in relation to this issue are mixed, however, and this is an issue which requires clarification.

⁶² The Acts give a wide meaning to 'processing', defining it as 'performing any operation or set of operations on the information or data, whether or not by automatic means, including – (a) obtaining, recording or keeping the information, or data, (b) collecting, organising, storing, altering or adapting the information or data, (c) retrieving, consulting or using the information or data, (d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or (e) aligning, combining, blocking, erasing or destroying the information or data.' See fn 64.

⁶³ This is the advice also of the EuroSOCAP guidelines (fn 12 at 19), which state that 'Where someone intends to render information genuinely anonymous, they can best ensure that they act legally and ethically by informing patients and/or their legal representative of their intention to do so and the effect that this will have, specifically on the ability of patients to access their data and to know what it is being used for (and hence to object to such uses). This is because the Data Protection Directive requires data subjects to be informed of the purposes of all processing of personal data and rendering data anonymous is itself a process performed on personal data. Furthermore, such prior informing should not be used as an excuse not to inform data subjects of the purposes of intended processing of data after rendering it anonymous. Anonymisation should be used in situations where that data does not need to be kept in personal form and it is not known for what purposes it might be used.'

Comment 1

The issue of whether or not the process of anonymisation is 'processing' within the meaning of the Directive and Acts requires clarification. Further commentary on this issue from the Data Protection Commissioner and/or the Article 29 Data Protection Working Party would be welcome and useful.

Recommendation No. R (97) 5⁶⁴ states that 'An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as anonymous.' Recital 26 also emphasises the effort involved in identifying a person as being a factor in deciding whether data is identifiable. The Working Party states that ' "Anonymised data" would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible.'⁶⁵

The Court of Appeal⁶⁶ attempted to deal with this issue, albeit not in the context of research. In doing so it disagreed with the contention that 'proposed anonymisation of the information...will...under the very wide definition of "processing"...constitute the processing of data concerning a patient's health...', preferring the contention, taking into account Recital 26, that:

...the directive can have no more application to the operation of anonymising data than to the use or disclosure of anonymous data (which, of course by definition is not 'personal data' and to which, therefore, the directive...has no application)...I would have to say that common sense and justice alike would appear to favour [this] contention. By the same token that the anonymisation of data is in my judgment unobjectionable here under domestic law, so too, I confidently suppose, would it be regarded by other Member States. Of course the processing of health data requires special protection and no doubt the 'erasure or destruction' of such data is included in the definition of processing for good reason: on occasion it could impair the patient's own health requirements. It by no means follows, however, that the process envisaged here should be held to fall within the definition: on the contrary, recital 26 strongly suggests that it does not.⁶⁷

⁶⁴ Committee of Ministers, *On the Protection of Medical Data*, 1997.

⁶⁵ *ibid.*, at 21.

⁶⁶ *Source Informatics* case, discussed in Chapter 1.

⁶⁷ *Source Informatics* case at 798–9. However, Casabona offers a different interpretation, stating that 'Personal data which is intended to be subjected to an anonymization process should legally be considered as personal data. Indeed when the anonymization has not taken place the data must be considered as personal data in the terms expressed by the Directive. Therefore it is data that should be subjected to all the principles of protection of the Directive. The consent of the interested person should be required in order to subject his or her data to the anonymization process, and he or she should be informed of the use-once the anonymization is made – to which his or her data will later be put. Data could be exempted from this duty of information to the data

The recitals are clearly of some juridical value as seen in the *Source Informatics* case. In relation to the recitals, especially Recital 26, Casabona⁶⁸ states:

...what is the juridical value of the Recitals of the Directive in comparison with the Articles? Are they obligatory, or do they only possess an interpretive or explanatory value in relation to the Articles? Undoubtedly, nobody would argue that the preamble lacks juridical value, that it is a merely rhetorical or aesthetic part of the Directive as it does not appear within the preambles of the internal laws. Even attributing only an interpretive value to the preamble, in relation to the issue at hand, Recital 26 does not seem to contradict Article 2(a) openly, but rather to expand on its contents. But it does have restrictive effects on what should be understood as 'identifiable people's data' because it adds that 'account should be taken of all the means likely reasonably to be used' to identify a person. When those means are not reasonable, the person will no longer be considered legally identifiable and the data will move into the category of anonymous data.

There has been a mixed reception to the *Source Informatics* decision, much of it critical. The indication from the discussion above may lend some support to Court's 'common sense and justice' approach in relation to this aspect of the decision but this remains to be seen.⁶⁹ Such an

subject when it is to be used to carry out scientific research (or research with historical or statistical ends) and the execution of the duty is impossible or demands disproportionate effort.' 'Anonymization and Pseudonymization: The Legal Framework at a European Level' in: Beylerveld D. *et al. The Data Protection Directive and Medical Research Across Europe* (Ashgate, 2004) at 48. Of course, no such exemption could have been available to Source Informatics as they were not conducting medical or scientific research. It was clearly commercial in nature. It should be further noted that the PRIVIREAL recommendations (at (c)) to the European Commission propose that 'The Commission issue guidance to discourage the use of the term "anonymisation" in favour of detailed statements about the form in which data is to be kept with particular attention being placed upon identifiers that have been removed but that can still be linked to the data.' At: <http://www.privireal.org/content/recommendations/#Recc>. The EuroSOCAP guidelines, at fn 13, also state that 'Thus, for example, where a researcher holds data in a form that does not enable the researcher to identify the data subject, but someone else holds a code that enables that person to do so, the processing done by the researcher is not processing of data rendered anonymous. However, it is not unknown for researchers to claim that they are processing anonymised data where others, or even they themselves, can identify the data subject by various straightforward means. For example, researchers usually describe any data that does not have the subject's name attached as anonymous. In practice, designating data as "anonymous" is a value judgment, and researchers should not use the term at all, but simply describe the form in which the data will be kept and processed, leaving it to the Ethics Committees and data subjects to decide what significance that has.'

⁶⁸ Casabona, *ibid.*, at 39.

⁶⁹ IMS Health (a company which collects data) in their submission also state 'Should the definition of "processing" under the Directive 95/46/EC actually cover the act of anonymisation? Clearly the Directive does not apply to personal data rendered anonymous. Recital 26 states that 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. A purposive view of this Recital leads one strongly to the opinion that the Directive should have no more application to the operation of anonymising data than to the use or disclosure of anonymous data. In fact, this is the exact view expressed by the judge, LJ Simon, in the UK court case...*Source Informatics*...' European Commission Review of EU Data Protection Directive, 2002 at 4. However, in relation to the decision, Lowrance notes that 'The arguments were cast so broadly, though, with everything from adequacy of the anonymisation, to

approach seems to also be emphasised by the Working Party which, while noting the importance of the fundamental rights and freedoms of individuals, states that:

It is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data. National Data Protection Supervisory Authorities play an essential role in this respect in the framework of their missions of monitoring the application of data protection law, which involves providing interpretation of legal provisions and concrete guidance to controllers and data subjects. They should endorse a definition that is wide enough so that it can anticipate evolutions and catch all 'shadow zones' within its scope, while making legitimate use of the flexibility contained in the Directive.⁷⁰

The case study overleaf, in relation to clinical trials and medical data, is provided by the Working Party to demonstrate these points:

implied consent by patients, to the European Convention on Human Rights, to doctors' conversations with drug sales representatives, being brought up, that it is not evident that the Source Informatics case set much useful precedent.' *Learning from Experience: Privacy and the Secondary Use of Data in Health Research* (Nuffield Trust, November 2002) at 17. Additionally, Jackson in her work is critical of the of the decision, stating that 'Even if the law is clear that the disclosure of anonymized records is not a breach of confidence, the process of anonymization itself, undoubtedly involves the "processing" of sensitive personal data, and will therefore be subject to the Data Protection Act....this must be done fairly and lawfully...if the patient has not specifically consented to the anonymization, it would have to be established that it was "necessary"...and done for medical purposes' *Medical Law: Text, Cases and Materials* (OUP, UK, 2006) at 350.

⁷⁰ Working Party, *op. cit.*, at 5.

Box 1: Case study of clinical trials and medical data

The medical professional/researcher ('investigator') testing the medicines collects the information about clinical results on each patient, earmarking him with a code. The researcher provides the information to the pharmaceutical company or other parties involved ('sponsors') only in this coded form, as they are only interested in biostatistical information. However, the investigator keeps separately a key associating this code with common information to identify the patients in a separate way. To protect the health of patients in case the medicines turn out to pose dangers, the investigator is obliged to keep this key, so that individual patients may be identified in case of need and receive appropriate treatment.

The question here is whether the data used for the clinical trial can be considered to relate to 'identifiable' natural persons and thus be subject to the data protection rules. ...to determine 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. In this case, the identification of individuals (to apply the appropriate treatment in case of need) is one of the purposes of the processing of the key-coded data. The pharmaceutical company has construed the means for the processing, included the organisational measures and its relations with the researcher who holds the key in such a way that the identification of individuals is not only something that *may* happen, but rather as something that *must* happen under certain circumstances. The identification of patients is thus embedded in the purposes and the means of the processing. In this case, one can conclude that such key-coded data constitutes information relating to identifiable natural persons for all parties that might be involved in the possible identification and should be subject to the rules of data protection legislation. This does not mean, though, that any other data controller processing the same set of coded data would be processing personal data, if within the specific scheme in which those other controllers are operating re-identification is explicitly excluded and appropriate technical measures have been taken in this respect.

In other areas of research or of the same project, re-identification of the data subject may have been excluded in the design of protocols and procedure, for instance because there are no therapeutic aspects involved. For technical or other reasons, there may still be a way to find out to what persons correspond what clinical data, but the identification is not supposed or expected to take place under any circumstance, and appropriate technical measures (e.g. cryptographic, irreversible hashing) have been put in place to prevent that from happening. In this case, even if identification of certain data subjects may take place despite all those protocols and measures (due to unforeseeable circumstances such as accidental matching of qualities of the data subject that reveal his/her identity), the information processed by the original controller may not be considered to relate to identified or identifiable individuals taking account of *all the means likely reasonably to be used by the controller or by any other person*. **Its processing may thus not be subject to the provisions of the Directive.**

A different matter is that for the new controller who has effectively gained access to the identifiable information, it will undoubtedly be considered to be 'personal data'.

The Irish Data Protection Commissioner in November 2007 issued the *Data Protection Guidelines on Research in the Health Sector*. The issue of whether the operation of anonymisation is processing is not addressed specifically. Nevertheless, the guidelines state:

Of course, where patient identifiable data is not required, which would likely be the case in a large number of situations, it is strongly recommended that patient data be anonymised before it is accessed for secondary research or clinical audit purposes.

Irrevocable anonymisation of personal data puts it outside data protection requirements as the data can no longer be linked to an individual and therefore cannot be considered to be personal data. Ideally such anonymisation of data for research purposes should be an automatic process performed as patient data is processed through IT or manual systems, whichever is the case. Where patient data is anonymised, there is no need from a data protection perspective to seek the consent of patients for the use of the data for research and clinical audit purposes...

However, in the discussions above, the opinion has been expressed that in looking at identifiability, irrevocably anonymised personal data will clearly fall outside the remit of the Acts as there would be no means 'likely reasonably' to be able to identify an individual. Nonetheless, that may also be the case with other types of anonymised data. However, it is vitally important that researchers understand the proper meaning of the terminology. The table below gives an example of the many different terms that are used in relation to this issue:

A concordance of terminologies

(Lowrance, *Learning from Experience: Privacy and the Secondary Use of Data in Health Research*. Nuffield Trust, 2002)

identified or identifiable	key-coded	non-identifiable
personal	reversibly de-identified	irreversibly de-identified
nominative	linked anonymised	unlinked anonymised
	Pseudonymised	Unidentifiable
	pseudoanonymised	Anonymous
	Coded	
	Masked	
	Encrypted	

In accordance with the above discussion, the following general comments can be observed in relation to identifiability and whether data is personal data:

Comment 2

Where research can be conducted on anonymous data, this is the most desirable option as such data is unidentifiable and the Acts do not apply to it. Researchers should attempt to ascertain whether it is possible to receive data in this anonymous format. The research participant's consent is irrelevant here as he/she cannot be identified. Receipt of data in this format may not always be possible or desirable.

Comment 3

If a researcher receives identifiable data, where possible, attempts should be made by the researcher to render the data as anonymous (make unidentifiable) or anonymise (make indirectly identifiable e.g. by key-coding or pseudonymising) the data at the earliest stage possible. Whilst opinions differ, the Acts may not apply to such processing, i.e. the operation of rendering anonymous or anonymising data, and such processing should be permissible without the consent of individuals. The techniques utilised to render anonymous/to anonymise should be accredited/approved/peer reviewed and must themselves ensure safeguards which protect confidentiality and privacy.

Comment 4

If a researcher receives anonymised data or anonymises the data (which is potentially capable of being identifiable), this may, in certain circumstances, be regarded as unidentifiable data (by examining and carefully assessing the means likely reasonably to be used by the data controller, e.g. the unreasonable time, manpower/personnel required and expense, that would be involved in identifying individuals, and the actual purpose of the research). Where the purpose is to ultimately identify individuals from the data, such data will be personal data. Taking into account at least these factors, and applying the principle of proportionality, data may be adjudicated to therefore be unidentifiable in certain circumstances. Thus, the Acts will not apply to it. Where the Acts do not apply, laws in relation to privacy and confidentiality may still be applicable.

2.3 Overview of sections 2, 2A–2D and the exemptions: Main obligations at issue

The general obligations in relation to personal data are dealt with in section 3 of the amendment Act (amending section 2 of the Principal 1988 Act) and processing is dealt with in section 4 of the Act. It provides for the addition of four new sections — 2A–2D — to the 1988 Act. There is now therefore what could be described as a 'layered' process,⁷¹ when examining what obligations data controllers and processors have in Ireland. The main words of importance are highlighted in bold.

2.3.1 Step 1: section 2 (keeping and processing); section 2d (fair processing)

Section 2: 1st General Obligation

The first general obligations are in relation to the keeping and processing of 'personal data' whereby section 2(1) states that those are:

A data controller shall, as respects personal data kept by him or her, comply with the following provisions:

⁷¹ These are described as List 1 and 2 by Lennon, *op. cit.*, and also as 'steps': see further for a general overview, Sheikh AA. 'The Data Protection (Amendment) Act, 2003: The Data Protection Directive and its implications for medical research' in Ireland *Eur. J. Health Law* 12: 357 (2005) at 359.

- (a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be **processed, fairly**
- (b) the data shall be accurate and complete and, where necessary, kept up to date,
- (c) the data–
 - (i) shall be **kept only for one or more specified, explicit and legitimate purposes,**
 - (ii) shall **not be further processed in a manner incompatible with that purpose or those purposes,**
 - (iii) shall be adequate, relevant and **not excessive in relation to the purpose or purposes for which they were collected or are further processed,** and
 - (iv) **shall not be kept for longer than is necessary** for that purpose or those purposes,
- (d) **appropriate security measures** shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

First exemption: Further processing/research exemption

It is important to note that the first exemption relevant to research appears in this section. Section 2(5) states that:

- (a) Subparagraphs (ii) and (iv) of paragraph (c) of the said subsection (1) do not apply to personal data kept for **statistical or research or other scientific purposes,** and the keeping of which complies with such requirements (if any) as may be prescribed for the purpose of **safeguarding the fundamental rights and freedoms of data subjects,** and
- (b) the data or, as the case may be, the information constituting such data shall **not be regarded for the purposes of paragraph (a) of the said subsection as having been obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained, if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject...**

The words 'specified' and 'explicit' are important and seem to indicate that the purpose of the data should be revealed clearly to subjects. The ordinary meaning of the word 'explicit' is the meaning an Irish court is likely to attach to a word, utilising the judicial canons of interpretation. Thus, looking at the definition of 'explicit', it is stated to be 'expressly stated,

leaving nothing merely implied; stated in detail.⁷² Section 2(D) (below) goes on to state that in addition to the keeping of data for an expressly stated purpose/s, the intended purpose/s of the data must be revealed to the data subject.

This first exemption may be a very important section in relation to any statistical, research or scientific purposes as it has potential ramifications for personal data utilised for a secondary use.

It seems to be case that, **in principle, personal data could be processed for a secondary purpose which was not originally considered but only if such secondary use cannot cause damage or distress to data subject.** It is to be noted that the words used in the section refer separately to the activities of statistical or research or other scientific purposes (in comparison to S2D (4) which refers to 'statistical purposes or for the purposes of historical or scientific research'. No definition of 'research' or 'scientific research' or of 'scientific purposes' is given in the Act. However, it is to be noted that the word 'medical' is not utilised in this section whereas it is later in the Act which suggests that there may be a deliberate distinction between 'scientific research' or just 'research' in this section and 'medical research' in the later section.⁷³ In this regard, the interpretation of the UK Information Commissioner of this equivalent section in the United Kingdom is that it will only apply to medical research on records involving individuals who are no longer being treated. This, however, is criticised by the Academy of Medical Sciences which states that:

Although this would appear to provide some help to researchers, in practice it is extremely difficult to make a clear distinction between current and old records and this statement [from the Information Commissioner's Office (ICO)] narrows the categories of research that can be supported under Section 33 considerably.

Consequently, the Working Group does not support the interpretation of the ICO. Instead, we strongly endorse the view that the Section 33 exemption was clearly designed to allow further data processing for research purposes to be carried out without revisiting fair processing requirements, providing that the processing is unlikely to cause substantial damage or distress and is not used to support decisions taken concerning the individual. We believe this should apply to both current and old records.⁷⁴

⁷² Concise Oxford Dictionary, 1990.

⁷³ Madden and McDonagh state that this exception applies only to research purposes and not treatment. 'Implementation of Directive 95/46/EC in relation to Medical Research in the Republic of Ireland' in: Beyleveld *et al.* (eds) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe* (Ashgate, UK, 2004) at 179.

⁷⁴ *Personal Data for Public Good: Using Health Information in Medical Research: A Report from the Academy of Medical Sciences* (UK, J2006) at 26.

The Directive at Recital 29 in relation to historical, statistical or scientific purposes states that safeguards must be provided to rule out the use of the data 'in support of measures or decisions regarding any particular individual'. Thus, the results of this research must be unidentifiable. This also seems to accord to the provisions of the Statistics Act 1993, as discussed in Chapter 1 earlier.

The provisions of section 5(h) should also be borne in mind here. section 5 restricts an individual's right of access to records and section 5(h) states that rights of access do not apply to personal data:

...kept only for the purpose of preparing statistics or carrying out research if the data are not used or disclosed... for any other purpose and the resulting statistics or the results of the research are not made available in a form that identifies any of the data subjects.

Thus, in relation to the UK equivalent of this exemption section, the Information Commissioner has stated that:

Where the exemption applies:

The further processing of personal data will not be considered incompatible with the purposes for which they were obtained.... ;

Personal data may be kept indefinitely... ;

Subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form that identifies the data subject.⁷⁵

Section 2d

In looking further at what 'fair processing' is, section 2(D) states that the data processor must ensure, **so far as practicable**, that the following **information be provided** to the data subject:

- (a) the identity of the data controller
- (b) if he or she has nominated a representative for the purposes of this Act, the identity of the representative
- (c) **the purpose or purposes for which the data are intended to be processed**, and
- (d) any other information which is necessary, having regard to specific circumstances in which the data are or are to be processed, to enable processing in respect of the data to be fair to the data subject such as information as to the recipients or

⁷⁵ fn 95 at 12.

categories of recipients of the data, as to whether replies to questions asked for the purpose of the collection of the data are obligatory, as to the possible consequences of failure to give such replies and as to the existence of the right of access to and the right to rectify the data concerning him or her.⁷⁶

Second exemption: 'Fair processing information' exemption

However, section 2D(4) states the exemption:

The said subsection...does not apply— (a) where, in particular for processing **for statistical purposes** or for **the purposes of historical or scientific research**, the provision of the information specified therein **proves impossible** or would **involve a disproportionate effort**...⁷⁷

According to section 2(D)(4), if not obtaining information from the data subject but from another source then the data subject should know of the identity of the representative of the data controller and name of the original data controller and the categories of data concerned. However, if this is for purposes of statistic/historic/scientific research and this information would be impossible to provide or would involve a disproportionate effort then the information does not have to be provided once any conditions are complied with as specified by the Minister after consultation with the Data Protection Commissioner (none such exist).

The 'disproportionate effort' might entail, *inter alia*, factors such as (i) the nature of the data and the effects of providing the information; (ii) the number of data subjects; (iii) the age of the data;⁷⁸ (iv) time and cost involved; (v) the entire circumstances of the situation. In relation to such factors, the UK Information Commissioner has stated that 'The above factors will always be balanced against the effect on the data subject and in this respect a relevant consideration would be the extent to which the data subject already knows about the processing of his or her personal data by the data controller.'⁷⁹

⁷⁶ Article 5 of Recommendation No. R (97) 5 also states in relation to information and the data subject that: '5.1. The data subject shall be informed of the following elements: *a.* the existence of a file containing his/her medical data and the type of data collected or to be collected; *b.* the purpose or purposes for which they are or will be processed; *c.* where applicable, the individuals or bodies from whom they are or will be collected; *d.* the persons or bodies to whom and the purposes for which they may be communicated; *e.* the possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal; *f.* the identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised. 5.2. The data subject should be informed at the latest at the moment of collection. However, when medical data are not collected from the data subject, the latter should be notified of the collection as soon as possible, as well as – in a suitable manner – of the information listed under Principle 5.1, unless this is clearly unreasonable or impracticable, or unless the data subject has already received the information.'

⁷⁷ These words are identical in the Directive at Article 11 (2).

⁷⁸ These two factors (ii) and (iii) are both noted in Recital 40 of the Directive.

⁷⁹ fn 95 at 9.

In these circumstances where the provision of information proves impossible or involves a disproportionate effort, it may be the case that consent cannot be obtained for these very reasons.

Consent and, if this is not possible, then anonymisation, are the best mechanisms for the protection of individuals.

The Data Protection Commissioner has stated this in his latest guidelines⁸⁰ that:

In very limited circumstances, where personal information is deemed integral to the success of a research project and where capture of consent is not possible for specific reasons, then the research can only be undertaken by the data controller itself with appropriate safeguards for the confidentiality of the patient information in place.

In relation to historical data, the guidelines go on to state:

In relation to personal data of a historical nature where no consent is in place for its use for research purposes, any access by a person or entity external to the data controller must be undertaken in the context of the Data Protection Acts. In particular, the data should be anonymised by the data controller prior to allowing access to the data to any external researcher. If access to patient identifiable information is required, or it is not possible to anonymise the information, every effort must be made to contact the persons involved and seek their consent by the data controller. If having undertaken all the above, access is still anticipated by a health professional or person otherwise owing a duty of confidentiality that is not an employee of the data controller, an appropriate data controller to data processor contract will need to be put in place stipulating the conditions attaching to such access.

However, these measures may not in all cases be either possible or appropriate in all types of research. In this regard, the document from the Canadian Institutes of Health Research *Secondary Use of Personal Information in Health Research: Case Studies*⁸¹ provides a useful

⁸⁰ *Data Protection Guidelines on Research in the Health Sector* (Data Protection Commissioner, 2007) at 14.

⁸¹ Canadian Institutes for Health, 2002 at 8–9. In relation to human biological samples, the Irish Council for Bioethics in their report, fn 3, at 6, state 'Where archival biological material was obtained from persons for research or clinical purposes, for which consent may not have been given or was not adequate for the current proposed research, where existing material is individually identifiable (identified/coded), researchers should seek to obtain free and informed consent from individuals, or from an authorised third party, for the use of their archival biological material. Where it is not practicable to obtain consent, a Research Ethics Committee may waive the consent requirement, in which case it should take into account: (a) whether the overall benefit to research is real and substantial (b) the extent to which the proposed research may pose a risk to the privacy or well being of the individual (c) the nature of any existing consent relating to collection and storage and use of material (d) whether the research proposal is an extension of, or closely related to a previously approved research project (e) the justification presented for seeking waiver of consent, including the extent to which it is impossible, difficult or intrusive to obtain consent.'

summary of the issues pertaining to the use of research for secondary purposes. This states that:

...the ability to conduct health research, particularly research on health services and population health, depends heavily on large volumes of readily accessible, existing data. Such data may include information derived from: personal interviews; analyses of tissue samples; results of scientific tests; physician, hospital and laboratory records; birth and death records; billing claims and employee records. The case studies focus on examples of research using data that were originally collected for another purpose (secondary use of data). Such existing data are often found to be extremely useful for identifying and understanding problems, as well as for providing potential solutions.

Researchers who study health services or the health of populations rarely have any direct interest in knowing the specific identities of the people they study. Their focus is on aggregate trends. So, while personal information about identifiable individuals may be the source of data, this type of research is conducted with information that has either been made completely anonymous or has had as many identifiers as possible removed and replaced with encrypted codes. Indeed, many investigators conducting studies would not need any personal identifiers at all were it not for the need to consider the effect of important individual characteristics or to link data about individuals so as to construct histories over time.

In some cases, therefore, the possibility of linking de-identified data to other potentially identifying information remains crucial. This is necessary in order to:

- study the relationship between certain health determinants and health status;
- group together individuals on the basis of common characteristics such as age or geographic location or
- track individuals over time in order to study the evolution of certain diseases after long latent periods or to assess their progress through the continuum of health care.

Researchers should implement deliberate strategies that make it impossible (or at least extremely difficult) to determine the identity of an individual from the data they use. Current practices for anonymizing, de-identifying and linking personal information (whether carried out by the original data-holder before releasing the data for research purposes or by the researchers themselves once in possession of the data) tend to vary significantly according to what is considered 'identifiable'. The ongoing challenge will be

to reach agreement on what constitutes an appropriate degree of identifiability, recognizing that this concept will continue to evolve. Approaches for de-identifying and linking data need to achieve greater consistency to streamline efforts for meeting and continually improving best practices.

Consent

In clinical research studies, researchers directly interact with potential participants in well-defined protocols and provide them with the detailed information required for obtaining their informed consent. However, strict application of traditional consent procedures in health services and population health research raises problematic issues, particularly for retrospective studies that rely on already-existing, historical or archival data, including sample survey data. Among the factors that often make seeking consent impracticable, impossible or self-defeating in these particular types of studies are:

- the sheer size of the populations studied;
- the proportion of individuals who may have since relocated or died;
- the risk of introducing potential bias through the consent procedure itself thereby affecting the generalizability and validity of research results;
- the creation of even greater privacy risks by having to link otherwise de-identified data with nominal identifiers in order to communicate with individuals so as to seek their consent;
- the risk of inflicting psychological, social or other harm by contacting individuals and/or their families in delicate circumstances;
- the difficulty of contacting individuals directly when there are no ongoing relations with them;
- the difficulty of contacting individuals even indirectly through public means such as advertisements and notices and
- the undue hardship that would be caused by the additional financial, material, human, organizational or other resources required to obtain individual consent.

The Confidentiality & Security Advisory Group for Scotland also explains the problems:

Epidemiological studies often involve thousands of patient records but tend not to involve direct contact between a patient and a clinician nor to use named data except to link items from different sources that are then anonymised. It is expected that wherever possible people will know about such studies and that their data are likely to be included. However, the practical difficulties in contacting large numbers of individuals can result in consent not always being sought before patient identifying information is processed.

Population-based research like this often uses large data sets (of the kind which NHS

Scotland collects) in order to monitor new or important diseases and to assess the effects of treatment or discover the underlying causes of disease. Examples of this are the links between smoking and cancer; between thalidomide and birth defects; or the association between leukemia in children and radiation. We depend on this kind of research in detecting new diseases and in monitoring the safety of new drugs and treatments, eg prescribing drugs to prevent thrombosis following major surgery, or for a vaccine against HIV. For most of these purposes complete data are important because opting out, even by small numbers of people, can bias the results and lead to wrong conclusions.⁸²

An example of these issues can be seen from the following case study:

Box 2: Case Study: Historic Research into 'Disease A' to establish a disease register

Researchers wish to establish a disease register for 'Disease A' based on past records over 50 years. This may identify any links the disease has to certain environmental factors. It is known that current rates of the disease are on the increase but no reasons are known. Consent for this study of the medical records was not ever taken in the past as it was never envisaged. The data on this register, if submitted, cannot be anonymised or put in aggregate form and must remain identifiable as the results cannot be otherwise validated due to missed cases or over-counting. Whilst obtaining consent from individuals is not necessarily an impossibility in all cases, it may be very problematic as (i) in the light of disease suffered it is an extremely sensitive and emotional issue to discuss and may be damaging to them and to any future professional relationship between doctor and patient (ii) even if consent were obtained, it could, at a later date be argued that such consent may not have been valid as the individual was in no fit state to give a valid consent or that this could not be ascertained (iii) even if the consent were valid, refusals of consent may bias the outcomes of the research as the results may not represent a proper population representation. This research is clearly important and in the public interest of a defined but large group. There is no issue of the researchers wishing to adopt a paternalistic attitude to the provision of information; however, the situation demands sensitivity and it is argued the public interest demands the research.

This study demonstrates the difficulty that researchers may be confronted with. In such a situation, the public interest is not only in relation to an undefined category of individuals, but to those (i) who have suffered from the disease; (ii) who are/may still be suffering from the disease; and (iii) who may suffer from the disease in the future. Thus, here, the balance of competing interests is not just in relation to the consideration of a potential violation of privacy of a defined group as against a general vague public interest exception.

The Data Protection Commissioner has suggested that where the contacting of individuals is not possible and thus obtaining consent is not practicable, then 'consideration needs to be given to

⁸² *Protecting Patient Confidentiality* (2002) at 14. At: <http://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf>

appropriate notices in the media'.⁸³

This has been utilised in other jurisdictions and should be attempted where it is deemed appropriate by the researchers and a research ethics committee. The following case study on the secondary use of personal information in health research illustrated the difficulties when:

...obtaining express consent in the context of large studies on population health and/or health services can sometimes be impracticable to obtain. However, this does not prevent researchers from seeking alternative means for providing individuals with the opportunity to become engaged and/or opt-out of the research. Researchers could also find creative ways of consulting relevant communities and studying representative focus groups with a view to better understanding what might be concerns of the larger study population that need to be addressed in the research design. Below are... examples of alternative means of consultation employed by researchers when individual consent was impracticable to obtain.

Box 3: Case Study: Cancer and other problems associated with breast implants

The purpose of this study was to identify harmful health effects on women who received breast implants for cosmetic reasons between 1975 and 1989. Following the recommendations of the REB [research ethics board] that reviewed the research proposal, the researchers in this case initiated a general information program that publicized the study aims and methods at professional meetings, through women's interest groups and in lay and scientific periodicals and newspapers. Informational pamphlets were also distributed to 35,000 physician offices across Canada for display in patient reception areas. A toll-free, bilingual hotline was set up in order to provide more detailed information and to allow women to opt out of the research.

Secondary Use of Personal Information in Health Research: Case Studies Canadian Institutes for Health, November 2002 at 29

⁸³ fn 81 at 11.

Comment 5: The Research and Fair Processing Exemption

The provision of information and consent is the primary method of protecting the rights of individuals. This should be done wherever and whenever possible. Where provision of information and obtaining consent is not possible, consideration could be given to advertising in the press, if possible and appropriate – allowing potential participants to opt-out.

The research exemption will apply therefore to *historic research* (not on current patients – but see [iv] below) *on identifiable data for secondary purposes* (purpose for which data was not originally collected) where this further use will not cause damage or distress to individuals and where the provision of fair processing information proves impossible or involves a disproportionate effort. Whilst there is no mention of consent in these sections of the Act, by implication, consent therefore, cannot be obtained. Researchers should seek to protect the fundamental rights and freedoms of individuals. Researchers should consider anonymisation of the data where possible, in seeking to apply the research exemption.

Researchers must seek approval by a Research Ethics Committee (REC) and:

(i) Seek a waiver of consent from a Research Ethics Committee (REC).

(ii) The REC should take into account the potential damage/distress to individuals of the further processing and whether non-provision of information and consent is impossible or would involve a disproportionate effort. In doing so, it should take into account at least the following:

- (a) the purpose of the research and whether the overall benefit of the research is real and substantial and clearly outweighs any potential risk
- (b) the extent to which the proposed research may pose a risk to the privacy or well being of the individual
- (c) the nature of any existing consent or provision of information in relation to processing of data
- (d) whether the research proposal is an extension of, or closely related to any previously approved research project
- (e) the justification presented for seeking waiver of consent, including the extent to which it is impossible, involves a disproportionate effort, or if it is difficult or intrusive to obtain consent
- (f) whether for the purposes of maximising protection of individuals, anonymisation could be considered. Researchers must be able to justify why anonymisation should not/cannot be done
- (g) whether advertising in the media/press would be appropriate in the circumstances, allowing individuals to opt-out of the proposed study.

(iii) The results of such research must not identify data subjects.

(iv) Clarification should be sought from the Data Protection Commissioner in relation to whether the exemption only applies to old records. The sections speak of 'historic', 'scientific' and 'research' as separate categories. Thus, can the exemption also apply to current medical records where fair processing information cannot be given and where consent cannot be sought?

2.3.2 Step 2: section 2A (consent or...)

The second general obligation takes account of the provisions of Article 7 of the Directive and states that personal data shall not be processed unless, in addition to satisfying the conditions which must be complied with in section 2 (Step 1), at least one of the listed conditions must also be satisfied, i.e. (the most relevant to medical research are highlighted in bold):

- **where the data subject has given his/her consent⁸⁴ to the processing** or in cases where the data subject is under age or incompetent, consent has been obtained from an appropriate person where the giving of such consent is not prohibited by law (*subsection 2A(1)(a)*);
- **where processing is necessary** for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract or for compliance with a legal obligation to which the data controller is subject (*subsection 2A(1)(b)(i),(ii) and (iii)*);
- where processing is necessary to protect the vital interests (health/property) of the data subject (*subsection 2A(1)(b)(iv)*);
- where processing is necessary for the administration of justice, the performance of a function conferred on a person by law, performance of minister/government (*subsection 2A(1)(c)(i)–(iii)*) or;
- **for the performance of any other function of a public nature performed in the public interest** by a person (*subsection 2A(1)(c)(iv)*);
- where processing is necessary for the purposes of the legitimate interests of the data controller or by the third party or parties to whom the data are disclosed (*subsection 2A(1)(d)*).

2.3.3 Step 3: section 2B (consent explicitly given or...)

The third general obligation takes account of Article 8 of the Directive, and deals with the issue of 'sensitive personal data' (which includes personal data in relation to physical or mental health or condition or sexual life of the data subject) and, in an attempt to provide additional protection, the Acts state that sensitive personal data shall not be processed unless in addition to satisfying the conditions of sections 2 and 2(A), at least one of the additional listed conditions must also be met, i.e.:

⁸⁴ It should be noted that Article 7 of the Directive uses the words 'unambiguously given his consent'. As discussed earlier, a consent in law can be expressed or implied. In this situation, can an implied consent be 'unambiguous'? Since, an implied consent arises from the behaviour of the patient upon which a healthcare provider bases a reasonable belief of consent, an implied consent could be said to be unambiguous where that behaviour is clear to the healthcare provider upon which to base a belief of consent. The implication could be made on the basis of a lack of objection once relevant information has been provided in appropriate circumstances. This of course remains to be judicially tested.

- **the data subject's consent referred to in paragraph (a) of subsection (1) of section 2A (Consent in Step 2) is 'explicitly given' (*subsection 2B(1)(b)(i)*);**
- where processing is necessary for the carrying out of any right or obligation on the data controller imposed by law in connection with employment (*subsection 2B(1)(b)(ii)*);
- where processing is necessary to protect the vital interests of the data subject (health/property) where the consent cannot be given by the data subject or where such the data controller cannot be reasonably be expected to obtain such consent or where in order to prevent injury or damage to health or serious loss to another person/property, consent is unreasonably withheld (*subsection 2B(1)(b)(iii)*);
- where processing is carried out by a non-profit making body with a political, philosophical, religious or trade union aim where such processing relates solely to its members and with appropriate safeguards for fundamental freedoms of data subjects and where there is no disclosure to third parties without the consent of the data subject (*subsection 2B(1)(b)(iv)*);
- where processing involves data which have already been made public by the data subject deliberately (*subsection 2B(1)(b)(v)*);
- where processing is necessary for the administration of justice, the performance of a function conferred on a person by law, performance of minister/government (*subsection 2B(1)(b)(vi)*);
- where processing is required for obtaining legal advice or in connection with legal proceedings or prospective legal proceedings or necessary for the establishment, exercise or defence of legal claims (*subsection 2B(1)(b)(vii)*);
- **where processing is necessary for medical purposes and is undertaken by a health professional or another who owes a duty of confidentiality to the data subject (*subsection 2B(1)(b)(viii)*);**
- where processing is necessary for statistical purposes and subject to the Statistics Act, 1993 (*subsection 2B(1)(b)(ix)*);
- where processing is carried out in the course of electoral activities for the purpose of compiling data on people's political opinions (*subsection 2B(1)(b)(x)*);
- **where processing is authorised by regulation for reasons of substantial public interest (*subsection 2B(1)(b)(xi)*);**
- where processing is necessary in connection with taxes or duties (*subsection 2B(1)(b)(xii)*); or
- where processing is necessary in connection with a benefit, pension, allowance etc. (*subsection 2B(1)(b)(xiii)*).

Definitions of the terms 'health professional' and 'medical purposes' are provided in *subsection (3)*:

'health professional' includes a registered medical practitioner, within the meaning of the Medical Practitioners Act, 1978, a registered dentist, within the meaning of the Dentists Act, 1985, or a member of any other class of health worker or social worker standing specified by regulations made by the Minister after consultation with the Minister for Health and Children and any other Minister of the Government who, having regard to his or her functions, ought, in the opinion of the Minister, to be consulted.'

Third exemption: 'Medical purpose' alternative/exemption

The 'Medical Purpose' Alternative appears at section 2B(1)(b)(viii) and this may be a very important section in relation to both medical research and public health in the context of the use of data for prospective medical research as the section states that sensitive personal data can be processed **'where processing is necessary for medical purposes and is undertaken by a health professional or another who owes a duty of confidentiality to the data subject'**. Medical purposes is defined as including **'the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services'** (section 2B(4)).

Further definition of 'medical research' is not provided here. It is interesting to note that a wider definition of research, under the title 'health research' appears in Statutory Instrument (S.I.) NO. 305 of 2007, The Health Research Board (Establishment) (Amendment) (No.3) Order, 2007 which defines 'health research' as:

- research with the goal of understanding normal and abnormal functioning, at the molecular, cellular, organ system and whole body levels, including research into the development of new therapies or devices to improve health or the quality of life of individuals, up to the point where they are tested on human subjects;
- research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury;
- research with the goal of improving the diagnosis and treatment (including the rehabilitation and palliation) of human disease and injury and of improving the health and quality of life of individuals as they pass through the normal life stages;
- research with the goal of improving the efficiency and effectiveness of health professionals and the health care system through changes to practice and policy;
- research with the goal of improving the health of the population or of defined sub-populations through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status.

Is the above-mentioned exemption, however, a blanket exemption allowing the processing of sensitive personal data without a subject's consent for any health data?

The Academy of Medical Sciences states in its report that:

For the purposes of the Act, the implication is that where consent is the *only* justification a researcher has for health data processing, it must be explicit...

It goes on to state that:

Although the Act therefore provides for the use of data without consent for medical research carried out by *bona fide* researchers, other conditions remain. Importantly this exception applies only when the processing for medical purposes is '*necessary*'; a term that is not defined in the Act. (It can be argued that medical research that has been approved by a properly constituted ethics committee is, by definition, *necessary* since it would not otherwise be ethically appropriate to conduct it).⁸⁵

It is interesting to note that the words 'necessity' and 'medical research' are contained in both the UK 1998 Data Protection Act and in the Irish Acts. Neither word is, however, contained in Article 8(3) of the Directive. The Directive uses the words 'where processing of the data is *required* for the purposes of...' ⁸⁶ It remains to be seen whether this suggestion as to the meaning of 'necessity' (i.e. if approved by a research ethics committee) would be accepted. However, it then begs the question of the meaning of 'necessary' in the context of medical research. While one can talk of the terminology of necessity in the context of treatment – thus, non-elective and/or emergency treatment being necessary, the same terminology of necessity does not translate in the context of medical research, except perhaps in a public health crisis situation (e.g. pandemic/epidemic). However, in that situation, the 'substantial public interest' alternative is available.⁸⁷ Thus, if the suggestion that a possible meaning of 'necessity' could be 'approved by an ethics committee', it would be advisable that research ethics committees (REC) carefully consider and be satisfied with the justification and purposes of the research protocol being considered and that those are properly documented (see also Comment 5). In many cases, there may be different degrees of necessity. While many research protocols are desirable to the community at large as they may gather very useful information in any given field of medicine, they may not be understood to be 'necessary' in a lay person's understanding of the word, in terms of there being an imperative to carry out the research. However, it is of note

⁸⁵ At fn 75 at 25.

⁸⁶ Recital 33 states only that 'Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.'

⁸⁷ Reliance on this alternative is supported by Recital 34, which states that 'Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as **public health** and social protection...'

that other jurisdictions such as Sweden do include the acceptance of a protocol by a research ethics committee in the manner discussed above subject to a 'benefit to society versus risk to individual' consideration.

Thus, the Swedish Personal Data Act (1998:204) states at section 19:

Sensitive personal data may be processed for research and statistics purposes, provided the processing is necessary in the manner stated in Section 10 and provided the interest of society in the research or statistics project within which the processing is included is manifestly greater than the risk of improper violation of the personal integrity of the individual that the processing may involve.

If the processing has been approved by a research ethics committee, the prerequisites under the first paragraph shall be deemed satisfied. Research ethics committee means such special body for consideration of research ethics issues that has representatives for both the public and the research and that is linked to a university or a university college or to some other instance that to a very substantial extent funds research.

Comment 6

In this context, the words 'necessary for the purposes of medical research' require further clarification, but there exists precedence from other jurisdictions whereby the necessity criterion is satisfied if (i) the interests of society in the research is manifestly greater than the risk of improper violation of the personal integrity of the individual and (ii) there is approval by an REC.

Comment 7

In the absence of clarification, all RECs should in any event always consider in detail the purpose and justification of a protocol and document the balance of competing interests as stated above.⁸⁸

In relation to consent, the previous Data Protection Commissioner, in relation to the Directive and its practical implications for data-protection law in Ireland, had in 2002 stated on his website:

Under existing data protection law, there is no specific requirement to obtain people's consent before using their personal data. There is simply a requirement to obtain and use people's data fairly, and in many contexts this requirement does entail the consent of the individual. Article 6 of the Directive preserves the requirement to obtain and use personal data fairly. In addition, Article 7 adds a number of clear requirements, at least

⁸⁸ Also stated by Sheikh AA. In *Genetic Research and Human Biological Samples: The Legal and Ethical Considerations* (Health Research Board, 2002) at 61.

one of which must be met before personal data can be used. One of these requirements, set out in Article 7 of the Directive, is that the individual 'has unambiguously given his consent'. The other, alternative requirements include the need to comply with a contract involving the individual; the need to comply with a legal obligation; and the use of personal data for the data controller's legitimate interests, where these interests override the individual's fundamental right to data protection. In general terms, it would appear that the Directive will, in many circumstances, shift the balance in favour of obtaining clearer, more unambiguous consent from individuals than has been the case up to now.

Sensitive personal data

At present, Irish data-protection law makes special provision for the handling of 'sensitive' categories of personal data, namely data relating to:

- racial origin
- political opinions or religious or other beliefs
- physical or mental health
- sexual life, or
- criminal convictions...

Article 8 of the Directive provides extra safeguards, which are additional to the data-protection requirements set out in Articles 6 and 7, for the handling of sensitive data...Such conditions include: where the individual has given his or her explicit consent... The prohibition on the use of 'sensitive data' does not apply to the medical and health-care sector, although of course the general data protection provisions of Articles 6 and 7 still apply.⁸⁹

This being the case, this would suggest that if the 'medical purpose' exemption/alternative were successfully relied on, whilst an explicit consent would not be required (Step 3 explicit consent), the exemption would *not* seem to remove the obligation of obtaining a consent (Step 2 consent).

Comment 8

Thus, for the processing of *prospective identifiable health research data for medical research* (Step 1) the data must be processed fairly (kept for specific purpose/s and ensure provision of information); and (Steps 2 and 3) the consent sought at Step 2 should be explicit, or process the data for necessary medical research or process in the substantial public interest. If processing is carried out under Step 3 without explicit consent, this does not mean that consent under Step 2 can be ignored (unless the data is attempted to be processed on the public interest criteria in both Steps 2 and 3 in which case consent will not be required).

The provision of an explicit consent will clearly satisfy all of the requirements and obligations on

⁸⁹ Irish Data Protection Commissioner: www.dataprivacy.ie (accessed on 18 November, 2002).

a data controller. It should also be noted that whilst it may not be necessary in specific circumstances, the flow of information in healthcare is also increasingly regarded as part of the consent process. It can be argued that to suggest that the requirement of consent in all medical research can be wholly dispensed with by the application of the medical purpose alternative in a blanket manner seems to be an over-simplistic reading of the legislative requirement. It also does not seem to accord with international ethical thinking and jurisprudence in relation to medical research, which requires the giving of full information to research participants. Thus, in the UK, the Department of Health has stated that:

The Government has made it clear that the fundamental principle governing the use of information that individuals provide in confidence to the NHS [National Health Service] is that of ***informed consent***. This is rooted in both legal and ethical requirements, but is also an essential element of an open and honest partnership between patients and the NHS that is based on trust.⁹⁰

Also, in relation to the UK's Data Protection Act, 1998, the Medical Research Council (MRC) has stated that:

The law recognises that research needs special freedom to use information in ways not foreseen when it was first collected, and to archive and re-use data. Research work that is not used as a basis for decisions affecting the individuals involved, and which is unlikely to lead to substantial damage or distress, is given special exemptions in these areas...The law also sets conditions on when 'sensitive personal data', such as information about health, religion, or ethnicity, can be processed. One condition is that the use of the data is necessary for medical purposes, (which are taken to include medical research and the management of healthcare services), *and* the processing is done by a health professional or a person with an equivalent duty of confidentiality. This condition is in addition to the need to conform to Common Law, and to other sections of the Data Protection Act. Despite the exemptions mentioned above, the Act is important for research. Fair processing requires that when Health Authorities, hospitals, and doctors know patient information will probably be used for specific research projects, at the time it is collected, they must tell patients this. Health professionals and researchers must give careful thought to whether their use of information might cause substantial damage or distress. Information gathered primarily for research but which will also be used to inform clinical decisions, or which will result in individuals receiving significant new health information about themselves, must comply with every part of the Act.⁹¹

⁹⁰ UK Department of Health. *Building the Information Core: Protecting and Using Confidential Patient Information, A Strategy for the NHS* (Information Policy Unit, 2001) at 1.

⁹¹ Medical Research Council. *Personal Information in Medical Research* (MRC, 2000) at 14–15.

In Ireland, in relation to the importance of consent as being central to the doctor–patient relationship, it has been stated that 'Informed consent is a critical element in the ethical conduct of research involving human subjects. It encompasses a procedure that begins with the initial contact and carries through to the end of the involvement of subjects in research'.⁹²

Further, in relation to data protection, the Irish College of General Practitioners (ICGP) states that:

The consent of the patient should be the guiding principle when obtaining personal health information and such consent should be informed to be meaningful. Accordingly, at the time of collecting personal health information, medical practitioners should take reasonable steps to ensure that the patient understands:

- what information is being collected;
- why the information is being collected;
- who within the practice will have access to the information;
- how the information will be used;
- the consequences of not providing the information;
- what third party disclosures are contemplated...⁹³

2.4 Types of consent

The Directive at Article 2(h) states that 'the data subject's consent' shall mean 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

A question that arises is whether an **implied consent** would suffice, especially if an explicit consent is not utilised. Implied consent is an accepted type of consent in law. The UK Information Commissioner states that:

...there must be some indication that the data subject has given his or her consent. This may be express (i.e. explicit) or implied. Express consent is given by a patient agreeing actively, usually orally or in writing, to a particular use or disclosure of information. Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information. For instance a patient who visits a GP for treatment may be taken to imply consent to the GP consulting his or her medical records to assist diagnosis. The Courts

⁹² Irish Council for Bioethics. *Human Biological Material: Recommendations for Collection, Use and Storage in Research* (Irish Council for Bioethics, 2005) at 23.

⁹³ The Irish College of General Practitioners. *Managing and Protecting the Privacy and Personal Health Information in Irish General Practice: An Information Guide to the Data Protection Acts for General Practitioners* (The Irish College of General Practitioners and the National General Practice Information Technology Group, 2003) at 10.

have not generally specified whether consent should be express or implied. It is clear, however, that for consent of any sort to be given, there must be some active communication between the parties. It would not be sufficient, for instance, to write to patients to advise them of a new use of their data and to assume that all who had not objected had consented to that new use. It is a mistake to assume that implied consent is a less valid form of consent than express. Both must be equally informed and both reflect the wishes of the patient. The advantage of express consent is that it is less likely to be ambiguous and may thus be preferred when the risk of misunderstanding is greater.⁹⁴

There are limited examples at common law in relation to this. In the Canadian case of *Allan v. Mount Sinai Hospital*⁹⁵ Linden J., described an implied consent stating:

It is not up to the patient to prove that he refused; it is up to the doctor to demonstrate that a consent was given. An actual, subjective consent, however, is not always necessary if the doctor reasonably believes that the patient has consented. Thus, if a patient holds up an arm for a vaccination, and the doctor does one, reasonably believing that the patient is consenting to it, the patient cannot complain afterwards that there was no consent: *O'Brien v. Cunard S.S. Co., Ltd.* (1891), 28 N.E. 266. Silence by a patient, however, is not necessarily a consent. Whether a doctor can reasonably infer that a consent was given by a patient, or whether he cannot infer such consent, and must respect the wishes of the patient, as foolish as they may be, always depends on the circumstances.

It is clearly the specific behaviour of the patient from which the consent will be inferred. A doctor cannot, for example, infer a patient's consent to surgery by the patient's mere presence in a hospital. Silence by itself from a patient may not be a consent. The situation will depend on the patient's behaviour upon which a healthcare practitioner can base a reasonable belief of consent on the basis that the patient understands what is about to be undertaken.

The British Medical Association (BMA) state that:

Consent can be verbal, written or implied by the acquiescence of a person who understands what will be undertaken. The provision of sufficient accurate information is an essential part of seeking consent. Acquiescence when a patient does not know what the intervention entails, or is unaware that he or she can refuse, is not 'consent'. Consent is a process, not a one-off event, and it is important that there is continuing

⁹⁴ *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998* (UK Information Commissioner, May 2002) at 15.

⁹⁵ 28 OR (2d) 356 at 363.

discussion to reflect the evolving nature of treatment.⁹⁶

However, in the context of **disclosure**, the latest BMA guidelines state:

As well as explicit consent, patient agreement can also be implied, signalled by the behaviour of an informed patient. Implied consent is not a lesser form of consent but it only has validity if the patient *genuinely* knows what is proposed and knows that he or she has a choice about participating. If not, it is no consent at all and some other justification will be needed for its disclosure. The concept of implied consent arose initially in the context of consent to treatment rather than consent to disclosure. It is easy to verify implied consent to treatment, if patients – having been informed of the reasons for a particular procedure – indicate by their actions that they agree to it. With implied consent to disclosure, verification is harder and doctors should take reasonable steps to ensure that this is obtained. Problems arise as it is often difficult to know with any certainty if patients really know either about the proposed sharing of information or their rights to opt out of it. **It should be noted that the more sensitive and detailed the data the more likely it is that express consent will be required e.g. sexual health information.**⁹⁷

In this regard, the Irish Data Protection Commissioner in his latest guidelines has stated the following in relation to the issue of consent and it is reproduced in full below:

The most straightforward way in which access to patient identifiable information for research or clinical audit purposes can take place in line with the requirements of the Acts, is with the consent of the person for the intended use.

...Provision of Explicit Consent:

Under the Data Protection Directive, the provision of explicit consent is a justification for the processing of sensitive data such as health data....What is being put forward here is a relatively simple model that every effort should be made to ensure that the patient knows what could happen to their data for purposes unrelated to their treatment and are given an opportunity to consent or refuse consent for such use. In this way, if any proposed use of a patient's data for purposes unrelated to their treatment would likely come as a surprise to them, then a new and separate consent should be sought. Again to be clear the Data Protection Acts support the flow of information in relation to the treatment/supportive care of individuals without the need for explicit consent and the

⁹⁶ BMA *Consent Toolkit*. 2nd edn, February 2003 at:
<http://www.bma.org.uk/ap.nsf/Content/consenttk2~card2>

⁹⁷ *Guidance on Secondary Uses of Patient Information* (Ethics Department, BMA, 2007) at 4.

guidelines are not intended to deal with such primary use of data.⁹⁸

... Specific

Where it is desired by a data controller to process a patient's information for a purpose other than the patient's treatment, it is strongly advocated, in line with European practice, that in so far as is practically possible, an informed and explicit consent be sought as soon as possible after a patient presents at a health facility rather than at a later point when access to that data might be sought. The exact administrative method for implementing such a practice would be a matter for the health facility in the first instance taking account of its own particular circumstances. The advantage of such an approach is that a health facility would set out in a fully transparent manner to the patient what it considers to be the permissible and desired uses of patient data. This should seek to highlight, based on past experience or known future plans, the specific purposes for which patient identifiable information may be accessed for purposes unrelated to the patient's treatment.

Such an approach would require each data controller to consider in a thorough manner what such potential uses might be and specifically capturing these in an appropriate consent supported by an informative patient leaflet. In this context, the freely given and informed consent of the patient would be obtained before the research is conducted, thereby complying fully with Data Protection obligations.

The manner and form in which such consent would be sought could vary from one health facility to another depending on its own circumstances. Such a consent would be by way of an 'opt in'. Patients should also be informed of their right to revoke their consent at a later date if so desired.

Although obviously of large benefit in terms of progressing matters from the current position where consent is not routinely sought at the outset, consent along the lines of that outlined above, will be unlikely to be sufficiently specific or cognisant of all potential uses of a person's data. Additional research initiatives, not envisaged at the time of seeking the initial consent, involving the use of patient data would need to be predicated on further specific consents going forward.

Such a situation will also likely arise where a patient presents to a health facility with different conditions on separate occasions. In such circumstances it would be unlikely that an initial consent for condition specific related research would cover research

⁹⁸ Future clarification on this point may be required to ascertain whether the non-requirement of explicit consent for primary healthcare, as is indicated here, is being done on the basis of reliance on the 'medical purpose' alternative. If that is the case, then while 'explicit consent' will not be required, 'consent' will still be required which is specific, informed and freely given.

currently related to the new condition also. In this respect, it must also be anticipated that patients will feel free to give consent for research on their data for some conditions but may refuse research on their data for other conditions where there may perhaps be extra sensitivity in relation to the condition or ethical considerations.

Such a system for routinely collecting and recording consent would also require a robust administrative system for correctly documenting patients' preferences to ensure that all subsequent access to their health data is fully in line with their stated wishes.

... Informed

The advantage of the above approach is that the patient would be informed at all times as to the possible uses of their data and can decide, based on the information provided, as to whether they would be agreeable to their data being used in such a manner. The health facility can decide, based on its own practices, as to the extent of information to be provided.

However, it is recommended that as much information as possible be provided to patients in the patient information leaflet. This would avoid the need, in all instances, to keep revisiting the patient to update their consent for specific additional purposes.

Such leaflets prepared by health facilities or GPs, as appropriate, should also provide assurances and details concerning all the safeguards in place designed to protect the patient's confidentiality. It is recommended that these leaflets outline how data may be disclosed in the future for the benefit of the patient, or for purposes not directly related to, or indeed completely separate from, the patient's own healthcare treatment. An outline of the types of research that may be conducted should be provided e.g. studies that use information from patient health records for the patient's own healthcare as opposed to studies that use information from patient health records as part of a survey. Patients should also be informed, if it is the case, that they could receive requests to participate in questionnaires or in randomised trials that focus on their particular health issues.

... Freely Given

Another key issue in terms of the means of gathering consent from patients is the requirement that such a consent be freely given. In this context it must be recognised that the patient may perceive themselves, in certain scenarios, to be in a vulnerable position as regards the treating medical team. Accordingly, it is strongly recommended that every effort be made to ensure that the context for seeking consent for further uses

of patient data be separated from any direct linkage with the patient's treatment.⁹⁹

Comment 9

Thus, for the processing of *prospective identifiable health research data for medical research* (Step 1) data must be processed fairly (kept for specific purpose/s and ensure provision of information); and (Steps 2 and 3) the consent sought at Step 2 should be explicit. The obtaining of explicit consent for prospective health research data for medical research will provide the best protection for individuals. In this regard, consent forms for research and data processing could be devised which envisage future secondary uses and options.

These options could be:¹⁰⁰

- (i) permitting the current research and processing of identifiable for this research only
- (ii) permitting the current research and processing of identifiable data and for that data to then be anonymised and used for future purposes (some explanation will have to be given in relation to possible anticipated future uses)
- (iii) refusing processing of the identifiable data for the current research and for anonymisation for processing of data for any future research (complete refusal)
- (iv) permitting processing of identifiable data for any study relating to the condition for which the data was originally collected, *provided they are contacted and their consent is obtained at the time of the research* and subject to the research being approved by a research ethics committee
- (v) permitting processing of identifiable or anonymised data for any study relating to the condition for which the sample was originally collected, *without further consent being required* and subject to the research being approved by a research ethics committee
- (vi) permitting processing of identifiable and/or anonymised data for any future unspecified research, *provided they are contacted and their consent is obtained at the time of the research* and the research is approved by a research ethics committee
- (vii) permitting processing of identified or anonymised data for any future unspecified research, *without further consent being required* and subject to the research being approved by a research ethics committee.¹⁰¹

Even with prospective research, problems can occur with consent. The following case study is an example:

⁹⁹ *Data Protection Guidelines on Research in the Health Sector* (Data Protection Commissioner, Dublin, 2007) at 7–9.

¹⁰⁰ These are adopted from the Irish Council for Bioethics, fn 3 at 2, and modified.

¹⁰¹ It will have to be clarified whether such an unconditional use offered by an autonomous individual can be permitted as in relation to keeping data. The Acts at section 2(1)(c)(i) require the data to be kept for 'one or more specified, explicit...purposes'. Thus, can such data, although given with a proper consent, be said to be specific? It could be argued that giving such an unconditional consent, is in itself, a specified purpose, i.e. processing for any future research, and thus should be permitted where the consent is valid.

Box 4: Case study: Access to GP medical records by a researcher

Researchers working with GP practices propose doing research on patient satisfaction in relation to primary care out-of-office hours service. They wish to collect a list of existing names and contact numbers from various GPs and then contact those on the lists in order to explain the research project. If the proposed participants agree to take part in the survey, they would be sent a questionnaire and consent to participation in the project was regarded as given when a survey was sent back, or refused, if the survey was not sent back. The research ethics committee refuses permission for this study on the basis that the proposal would breach the obligations of confidentiality and the Data Protection Acts, including the provision of names, addresses and contact numbers from the GP to the researchers, as consent for the use of this data must be taken at the first point of contact, i.e. when GPs take information from their patients as otherwise patients being contacted by researchers may think that the researchers have had access to their medical records and are using those records for a purpose they did not envisage or were not told about initially. The researchers claimed that to conduct such research in any other way would lead to a reduced participation rate. A suggestion was made that the researchers could be nominated by the GPs as 'data agents' in order to carry out the research. Does the Act allow this? Another issue that arises is on whom does the onus lie in deciding whether or not a research proposal is in accordance with the Data Protection Act?

The Data Protection Commissioner has made clear that in his latest report that:

...a data controller could be an individual such as a GP or other medical professional working in a private capacity who is responsible for collecting information in the context of the treatment of a patient. It is this data controller who is legally responsible for the processing of the data under the Data Protection Acts. For the avoidance of doubt this personal legal responsibility arises only where the individual is working and responsible for the collection of the data in that private capacity.¹⁰²

The Acts state the definition of disclosure to be:

'disclosure', in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data **but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties**; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed...

What is not clear is the intended definition of 'agent' in the Acts or of the words in bold especially in relation to the words 'his duties'. It probably makes more sense if the words 'his duties' relate to the duties of the agent within the course of his 'employment' or 'services' with the GP – for example, an agent locum doctor. Clearly, if a GP were to hire a researcher as

¹⁰² fn 81, at 7.

his/her agent, that agent's duties are not related to the work of the GP. Thus, the agency idea would not seem possible. In this scenario, it would seem, subject to clarification by the Commissioner, that the GP would be obliged to contact his/her patients and seek their consent to be contacted by the researcher. It has been observed that 'there is some evidence indicating that patients feel more obliged to participation if the approach comes from their own practitioner',¹⁰³ however, this potential sensation of obligation could be diminished if the GP forwarded a covering letter explaining the situation which included an information leaflet from the researcher, thus distinguishing the two entities. Other than this, it is difficult to see what other options exist in relation to the 'consent to consent' process, as cumbersome as it may seem, unless the substantial public interest ground was claimed, which may be difficult to satisfy in these circumstances.

It is also important that the 'circumstances' of consent be understood. Thus, as discussed earlier, providing information in relation to research at a time when a patient is about to undergo surgery, is likely to be questionable.¹⁰⁴ Further, the provision of information in an accident and emergency department for retention and processing of data may also not suffice with the requirements of the Acts. Thus, the Data Commissioner in 1997, in *Case Study 1/97*¹⁰⁵ found that the use of patient data that had been obtained in an accident and emergency department and that was then utilised for research purposes that had not been clearly indicated to a patient fell foul of the 1988 Act and that signs displayed in the department alerting patients that their data might be used in research, in this case, were not sufficient. The commissioner found that:

...for personal data to be fairly obtained, a data controller must make the data subject aware, directly and at the time his or her data are being obtained, of how such data may be used and to whom they may be disclosed, in order to get the person's informed consent to the uses and disclosures described. The hospital's second argument related to the notice which it had placed in the waiting area. In my view, the issue to be decided was whether this was an adequate way of informing patients that their information would be disclosed to the researchers. In different circumstances, it might have been. In this case, however, account ought to have been taken of the particular environment in which patients' data were obtained. Many patients presenting themselves at the casualty department of a hospital may be expected to be in a state of some anxiety or discomfort. Consequently, they may not be expected to be alert to matters not relating directly to their condition. In such circumstances there is a special need for the data

¹⁰³ fn 75 at 63.

¹⁰⁴ See fn 23, *Fitzpatrick* case and see further on this issue: Sheikh AA. 'Lessons for healthcare from litigation: 2007 – a busy time for Medical Law' (2007) 13, 2 *Medico-Legal Journal of Ireland (M.L.J.I.)*: 54–62 and at 87.

¹⁰⁵ Case Study 1/97 accessed on 18 August, 2005 at: www.dataprivacy.ie

controller to satisfy itself that any uses of the data which are unlikely to be anticipated by the data subject are fully explained. For this reason, I took the view that the intention to disclose should have been brought to the specific attention of the complainant before data relating to her were obtained. This was essential to ensure that she was in a position to make an informed choice whether or not to furnish her information for such a purpose.¹⁰⁶

Comment 10

The requirements for the provision of information for fair processing and consent (which should be integrated into a healthcare provider's existing systems, guidelines and protocols), may all be met by the following possible methods (in multiple languages), which should be used in combination:

- Detailed standard and research patient information leaflets (can also be part of the admission process e.g. for giving information in relation to processing issues such as administration, internal audit and quality control, risk management, payment and inter-team use of data).
- Posters.
- Information on websites.
- One-on-one consultations (for explicit consent this should be standard procedure).
- Consent forms (for explicit consent).
- In appointment letters and correspondence.¹⁰⁷

Fourth exemption: 'Substantial public interest' alternative/exemption

Article 8(4) of the Directive provides that 'Subject to suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions...either by national law or by decision of the supervisory authority.' In accordance with this, section 2B(1)(b)(xi) of the 2003 Act provides an alternative to the 'explicit consent' requirement where **'processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest.'**

This is a 'Step 3' alternative to an explicit consent. This was clearly designed for the purposes of public health reasons and reliance on this alternative for such public health reasons is supported by Recital 34 which states that 'Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection...'

¹⁰⁶ Case Study 1/97 at: www.dataprivacy.ie

¹⁰⁷ See further: Lennon, *op. cit.*, at 157–8, Data Protection Commissioner Guidelines as above in main text and at fn 81 and *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998* (UK Information Commissioner, May 2002) at 8.

This section could and should be used to allay the fears of those in the public health research sector who fear that:

Much epidemiological research and research into health economics would simply be impossible to conduct if completely anonymous data had to be used because updating, linking, or validating data is impossible without using codes.¹⁰⁸

Those voices are many:

Ideally, patients in a research study or audit should have given their consent to the use of data that preferably should not identify them directly. This consent can be implicit when a patient is aware of the disclosure and their right to refuse, yet makes no objection. Although explicit written consent is essential for most trials of any intervention, it is an unrealistic requirement of observational research and audit, particularly if these rely on huge quantities of previously collected data. Systematic bias could invalidate the findings of observational studies if people were excluded because they did not consent. For example, obtaining consent could be biased by age or gender, and by whether individuals are dead, untraceable, cognitively impaired, or deemed too distressed to be approached for their consent. Anonymised information is often not sufficient because patient identifiable data are required to avoid duplication and to follow up individuals indirectly....A blanket requirement for anonymisation of data, as well as informed consent from all individuals to use identifiable data about them, would jeopardise the methodological integrity of research and audit. This would not just hinder the progress of medical knowledge but might lead to completely incorrect conclusions. This would be against the public interest and make the process of clinical governance impossible...Ambiguous statutory regulations, contradictory guidance, and a vocal minority of objecting patients or those representing them will thwart observational research relying on patient identifiable data, audit, and clinical governance. Investigators must design studies appropriately and need to know that their use of existing, valuable datasets is legitimate. Ethics committees must review proposals consistently and should not be threatened with court action to determine where the public interest lies. Patients should be made aware of which data about them may be used for purposes which further the public interest and the understanding and management of their own disorder.¹⁰⁹

¹⁰⁸ Strobl J *et al.* 'Data Protection legislation: Interpretation and barriers to research' (2000) 321 *BMJ* 890–2 and also: Peto J. *et al.* 'Data Protection, informed consent, and Research' (2004) 328 *BMJ* 1029–30. Adams T. *et al.* 'Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent' (2004) 328 *BMJ* 871–4.

¹⁰⁹ Al-Shahi R & Warlow C. 'Using patient-identifiable data for observational research and audit' (2000) 321 *BMJ* 1031–2. See also: O'Neill O. 'Some limits of informed consent' (2003) 29 *J. Med Ethics* 4–7. Turnberg L. 'Common sense and common consent in communicable disease surveillance.' (2003) 29 *J. Med. Ethics* 27–9. Lachmann PJ. 'Consent and confidentiality – where are the limits? An

The following case study reflects these concerns:

Box 5: Case Study: Prospective research to establish a congenital anomaly register

Public health practitioners wish to establish a congenital anomaly register. This will be done by accessing records, the purpose for which was not initially disclosed and for which there may not be any previous consent. The data on this register cannot be anonymised or in aggregate form and must remain identifiable as the results cannot be otherwise validated due to missed cases or over-counting. Also, this is a longitudinal study which will operate over many years. Whilst obtaining consent from parents is not an impossibility, it may be very problematic as (i) in the light of the child having a congenital abnormality it is an extremely sensitive and emotional issue to discuss with parents and may be distressing and damaging to them, and to the professional relationship between doctor and patient. In addition, some of the children may have died; (ii) even if consent were obtained, it might, at a later date, be argued that such consent may not have been valid as the parent was in no fit state to give a valid consent; (iii) even if the consent were valid, refusals of consent may bias the outcomes of the research as the results may not represent a proper population representation. This research is clearly important and in the greater public interest and for the wider common good. There is no issue of the researchers/healthcare providers wishing to adopt a paternalistic attitude to the provision of information; however, the situation demands sensitivity and the public interest, it is submitted, demands the research.

For this type of research, it could be argued coherently that the 'medical purpose' alternative will be relied on as the medical research is necessary and thus no explicit consent is required to be sought. However, that still requires there to be a consent. Since that condition cannot be satisfied either, it could be argued that the public interest (Step 2) and substantial public interest (Step 3) are applicable and therefore no consent is required. However, this is subject to regulations as specified, of which none yet exist.

In 2002, the Medical Research Council in the UK stated that:

When consent is impracticable confidential information can only be disclosed without consent only if:

- the likely benefits to society outweigh the implications of the loss of confidentiality, so that it is clearly in the public interest for the research to be done;
- there is no intention to feed information back to the individuals involved or take decisions that affect them; and
- there are no practicable alternatives of equal effectiveness.¹¹⁰

introduction' (2003) 29 *J. Med. Ethics* 2–3. Haynes *et al.* 'Legal and ethical considerations in processing patient-identifiable data without patient consent: lessons learnt from developing a disease register' (2007) 33 *J. Med. Ethics* 302–7. Metcalfe *et al.* 'Low risk research using routinely collected identifiable health information without informed consent: encounters with the Patient Information Advisory Group' (2008) 34 *J. Med. Ethics* 37–40.

¹¹⁰ *Personal Information in Medical Research* (MRC, 2000) at 10.

It is for this type of research and situation that the UK introduced section 60 in the Health and Social Care Act, 2001. That Act enables the Secretary of State to support and regulate the use of confidential patient information in the interest of patients or the wider public good. Parliament agreed to the creation of this power to ensure that patient-identifiable information can be used, without the consent that should normally be obtained, where there is no reasonably practicable alternative. In particular, it cannot be practicable to rely upon patient consent or to work only with anonymised data. A case must be successfully made that the purpose for using patient identifiable information is in the best interest of patients or, alternatively, serves a wider public good. The process involves application to a REC and then scrutiny by the Patient Information Advisory Group (PIAG). If the PIAG advises, legal regulations may be considered such as the Health Service (Control of Patient Information) Regulations. However, a note of caution has been sounded by Case who states that 'It should now be apparent that informational autonomy is being afforded a far lower level of protection than physical autonomy.'¹¹¹

Moreover, in their report *Human Rights, Privacy and Medical Research: Analysing UK Policy on Tissue and Data* the Genetic Interest Group state that:

The government, civil servants, regulators, professional guidelines and academic commentators repeatedly emphasise the importance of confidentiality, privacy and consent. In contrast, they give very little attention to the importance of medical research, its similarities with clinical audit and its connections with evidence-based care. Nor is much scrutiny given to the finely balanced exemptions that were purposively included in data protection legislation and have been developed by the courts in common law decisions about confidentiality. As a result, the regulatory burdens imposed on research are crudely interpreted to be more demanding than the higher courts would likely have held if the questions had been litigated in court. These burdens are severely hampering scientific investigation, especially epidemiological research.

A further problem is that strict interpretation of the right to privacy protection can be self-reinforcing. If called upon to decide a dispute, the courts would ordinarily give deep consideration to guidelines published by the Department of Health, the NHS, the Office of the Information Commissioner, the Patient Information Advisory Group, the Medical Research Council, the General Medical Council or a combination of these. If a large number of these bodies suggest that there is a strict requirement to obtain explicit

¹¹¹ Case P. 'The rise and fall of informational autonomy in medical law' (2003) 11, 2 *Med. L. Rev* 208 at 232. Case does not inherently reject the Act, but is critical of the lack of safeguards. She states, at 236, that 'What is crucial, however, is that these "legitimate restrictions" [on a patient's autonomy] are surrounded by robust safeguards concerning who decides when autonomy can be restricted and the scope of such restrictions. Only then can inroads on informational autonomy be truly justified as in the public's interest.'

consent or to anonymise data fully, judicial assessments of what is 'reasonable', 'unconscionable', 'proportionate' or 'good practice' may be affected.¹¹²

For the establishment of national disease registers, the Data Protection Commissioner has stated that:

In relation to specific projects of national public health importance such as the National Cancer Registry, appropriate safeguards can be provided via legislation. It must still be emphasised however that all other data protection rights in terms of further processing, disclosure, access, security etc. will remain.¹¹³

Legislation currently exists in Ireland in the form of the Health (Provision of Information) Act, 1997 that allows for the compiling of information for the purposes of cancer-screening programmes and which is excluded from the data-protection legislation.

Similar legislation or regulations may have to be properly considered to ensure that work in medical and public health research which is clearly in the substantial public interest is not unduly hampered. Derogations of this nature are envisaged by the Data Protection Directive. It may be the case that legislation similar in intent (but perhaps not in its mechanics) to that in the UK may now fall to be considered. The matter could also be dealt with without the need for legislation. This is the option that has been adopted, for example in Scotland.¹¹⁴ However, whatever route may be taken, if inroads are made into informational autonomy (albeit on the basis of the 'public interest/good') any such moves will require wide-ranging consultation, debate and a need to learn from the lessons of other jurisdictions. The constitutional right to privacy must be respected and any legislation that may threaten it may of course be open to constitutional challenge in the courts. It may be the case that progress could be made on this front by the combination of (i) approval by a research ethics committee and (ii) notification and approval by the Data Protection Commissioner. However, such transfer of responsibility on under-resourced RECs may place burdens on such committees that cannot be lifted.

¹¹² Gillot J. Genetic Interest Group (2006) at 25.

¹¹³ fn 81 at 14.

¹¹⁴ *Protecting Patient Confidentiality* (The Confidentiality & Security Advisory Group for Scotland, 2002).

Comment 11

(i) The 'medical purpose' exemption will fall to be used in circumstances where data processing for prospective medical research on identifiable data will be argued to be necessary, but obtaining explicit consent will not be practicable or will defeat or seriously compromise the research proposed. The involvement and approval of research ethics committees will be required, but, they should also receive specialist training and education in the field of data protection.

(ii) The notification and approval of the Data Protection Commissioner should also be involved in this process.

(iii) Where necessary, legal advice should also be sought as issues involving the common law breach of confidentiality will also come into play. Any potential breach of confidentiality must be justifiable. It must be emphasised that the law of confidentiality and privacy has not yet considered a balance of competing interests involving a potential breach of privacy and confidentiality as balanced with the public interest in allowing access to identifiable patient data for medical research.

(iv) It may be advisable in the future to consider legislation similar to that in the UK in relation to limited access to patient identifiable data in research on limited grounds and in the public interest. However, it is crucial that if such a step were considered necessary, that a wide ranging consultation be carried to ensure that the lessons from other jurisdictions are learnt and considered.

(v) In other situations such as national disease registers, the 'substantial public interest' exemption/alternative will fall to be utilised in public health scenarios. The passing of regulations for all of these may/may not be practical in all situations, however, matters of this nature must be debated and considered on a case-by-case basis.

(vi) In the absence of further legislation or regulations, in cases of any doubt, researchers must contact the Data Protection Commissioner.

2.5 Conclusions

Whilst medical researchers maintain concerns over the Directive and transposing legislation, in various European Union (EU) Member States (including Ireland), the Directive and the Acts allow flexibility to a certain degree to enable Member States to mould legislation to answer these concerns by, for example, passing legislation subject to safeguards, which is in the public interest. There are inconsistencies amongst EU Member States. Some have opted for a more, it seems, liberal approach, for example, Sweden, in the application of the medical research exemption.¹¹⁵ Others, however, such as France and Germany, have opted for a less liberal approach. The lack of consistency has not helped in the interpretation of the Directive (see also Chapter 4).

¹¹⁵ This is discussed in some detail in Chapter 4. It should be noted that the PRIVIREAL Project has called for a number of clarifications and has made recommendations. At: www.privireal.org/content/recommendations/. It should be noted that some of these have been criticised by the UK Academy of Sciences, *op. cit.*, at 41.

Nevertheless, the exemptions are in place for a reason and they do not allow data controllers to by-pass their obligations to ensure that, prior to the processing of health and personal data, a subject gives his/her consent on receipt of information in relation to the data. Where such prerequisites are not possible, exemptions, subject to suitable safeguards, can be utilised.

There are, as seen above, concerns from the medical research community over the ramifications of the data-protection legislation. In addition, there is a growing call from the medical and scientific communities in relation to the need to recognise properly the growing 'public interest' of society's demand for better health. For example, the BMA, have commented recently on this:

Box 6: BMA Guidance on secondary uses of patient information

Although in the past the BMA has tended to espouse a fairly narrow definition of public interest, it recognises that, in the context of secondary use of information, public interest must be a balance between individuals' and society's rights and claims to confidentiality and the rights and claims of the whole of society to better health and to protection against threats to ill health. Any disclosure of identifiable information must be proportionate to the anticipated benefit and subject to good governance rules. To make such an evaluation requires consideration of:

- the degree of disclosure and the expected benefits for society
- the degree of intrusiveness for the patient
- the level of public awareness and acceptance of the disclosure

...what constitutes the public interest in any case is ultimately a matter for the law although in extreme cases where non-disclosure represents a serious threat to the health or welfare of individuals, e.g. child protection, it will almost inevitably be in the public interest to share information appropriately with third parties. However, in all other cases, unless it is absolutely clear that the disclosure is in the 'public interest' doctors would be well advised to adopt a cautious approach... **(Ethics Department, BMA, 2007) at 5**

A balanced approach to data protection can be achieved. It must from the outset realise a patient's primary right to privacy and then balance that primary right with the public interest in public health medical research in certain situations.

Achieving this balance will require wide consultation, new and improved practices, investment in new technologies and training. It may require new regulations. Some degree of patience to allow for the inevitable inconvenience of new practice must also be allowed. If this is accomplished within an overall, integrated health-information strategy then this will ensure a coherent and efficient approach to a complex area of law and medical practice that is essential in the longer-term interests of both patients and public health.

In these circumstances, the following suggestions to Irish healthcare providers and medical and public health research communities may assist in the further translation of data-protection law into practical medical policy.

2.6 Concluding comments

Comment 12

Provide greater information to patients in relation to their health data by the use of easy-to-understand patient information leaflets and improved consent forms which explain the use and potential uses of medical information. Healthcare providers should also include such information on websites. This will give patients and opportunity to understand their range of options in relation to the processing of their data and will therefore enable patients to give a valid consent to data processing. As consent in clinical care is increasingly recognised as a process and not a once-off event, the flow of information in relation to a patient's overall care should be increased by ongoing communication in any healthcare setting.

Comment 13

Discuss at a national level the appropriate utilisation of anonymisation techniques in medical research and public health work. A technical analysis and consideration and continuous monitoring of effective/best practice Privacy Enhancing Techniques (PETs) could be undertaken by agencies such as the Health Information and Quality Authority (HIQA) under its Health Information mandate. HIQA reports that:

The interim Authority undertook a considerable stakeholder engagement with key individuals and organisations across the system. It has also commissioned a research project that is looking at the information standards required for the inter-operability of systems as the information and communications technology systems become increasingly more refined across the health system.¹¹⁶

Such projects might consider the issue of PETs.

¹¹⁶ Annual Report of the interim Health Information and Quality Authority 2006/2007 at 16. Where it is also reported at 17 that, 'Dr Brian Meade represents the interim Authority on the National Standards Consultative Committee for Health Informatics, under the National Standards Authority of Ireland Act, 1997. This committee will contribute to the development of European and international standards for patient and hospital information systems and provide advice on national standards in this area.' The issue of information and health data sharing and unique health identifiers would also need to be examined to ensure standards of privacy are not compromised. Thus, e.g. currently the use of the PPS (personal public service) number and the 'sharing of information' in this regard is permitted for limited circumstances under the Social Welfare Act, 1998 at section 14 which states that: '(2) A specified body holding information may share that information with another specified body who has a transaction with a natural person relating to a relevant purpose, where the specified body seeking the information provides the personal public service number of the person who is the subject of the transaction and satisfies the data controller of the specified body holding the information that the information requested is relevant to the transaction for the said purpose between the person and the specified body seeking such information.
(3) A specified body may only seek information for the purposes of a transaction relating to a relevant purpose.
(4) Where information shared between one specified body and another is found to be inaccurate, the specified body on making the discovery shall confirm with the person the correct information and advise the other specified body of the amended information.
(5) A person who, other than for a transaction in respect of a relevant purpose, knowingly seeks or transfers any information held by a specified body relating to another, by using that other's personal public service number, shall be guilty of an offence.'

Comment 14

Clarity of language is important in the area of data protection to avoid confusion of meaning. Thus, the meaning of words such as 'anonymisation' should be clarified and standardised. Certain Member States such as Germany and Spain have clearly defined such terminology and Ireland should follow suit.

Comment 15

Encourage interdisciplinary debate, discussion and practice of data-protection principles and applications in medical research in various medical sectors and with RECs to ensure understanding, compliance and standardisation of key issues and their applications to research and in ongoing co-operation with the Irish Data Protection Commissioner to invoke the Statutory powers of the Office under section 14 of the 2003 Act in order that Codes of Practice be considered.

Comment 16

That the Minister (for Justice, Equality and Law Reform) and/or the Data Protection Commissioner consider passing specific legislation/regulation to exempt or partially exempt certain categories of public interest health data and the consent requirements in very specific cases and after proper consultation.

Comment 17

Engaging the public and providing information to them about medical research will be important in terms of a long-term public education plan. Lowrance refers to this as 'dialogue' with the public and states that, 'Among other things, dialogue over these matters will contribute to serving the 'fair notice' called for by the Data Protection Act.'¹¹⁷ In Ireland it has also been stated that:

Ongoing information, education and evaluation is needed to enable the dialogue necessary among the widest public audience, professionals and policy makers. Ultimately, research in the health context is itself a public resource. The public good that can be achieved through research can only develop and prosper through increased dialogue among all of the relevant stakeholders.¹¹⁸

The same report in relation to consent states that:

in relation to preferences for consent procedures, findings were equivocal with similar proportions supporting either general or specific consent. This study thus informs and can help to set an agenda for further communication with the public rather than opting for restrictive legislation, e.g. the option of specific consent only as a 'safe' bet in all circumstances.¹¹⁹

As also suggested by the UK Academy of Sciences:

'Researchers know that medical research in general, and research using personal data in particular, is highly regulated. The public, however, is largely unaware of these controls and the way in which the standards of research are maintained. This is a matter of concern for both the public and researchers alike. The advice we received indicates that the wider research community must itself engage with the public to raise awareness of the benefits of the research involving personal data and to demonstrate that high standards are consistently applied. Research funders, regulatory bodies and universities could do much in this area, and we encourage collaborative activity.... Charities with strong patient/user input could also play a particularly important role in more actively advocating the value of research using personal data. Ultimately, there is a need for... Departments of Health to undertake a programme of public engagement around these issues.'¹²⁰

¹¹⁷ Lowrance *op. cit.*, at 66.

¹¹⁸ Cousins *et al. Public Perceptions of Biomedical Research – A survey of the general population in Ireland* (Royal College of Surgeons of Ireland with the Health Research Board and the Department of Health and Children, 2005) at 61.

¹¹⁹ *ibid.*

¹²⁰ UK Academy of Sciences, *op. cit.*, at 72.

3 Records, disclosure and the deceased

3.1 Introduction

A question that often arises in medical research is whether the medical records of a deceased can be accessed or released for research purposes and whether the consent of the next-of-kin is required.¹²¹

This is a complex area of law and it cannot be said that there exists a clear answer to the query.

This short chapter attempts to set out the various positions and suggest a manner in which access to such records may be argued to be justifiable.

3.2 The data-protection issues

The Irish Acts state that “data subject” means an individual who is the subject of personal data’. However, it goes on to state that “personal data” means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.’

The Data Protection Directive at Article 2 states that “personal data” shall mean any information relating to an identified or identifiable natural person’.

The PRIVIREAL Project sought clarification on this point, stating:¹²²

This is not a question of ‘rights’ for the dead. The central issue is whether the Directive covers data that relates to a person who has died. It concerns whether duties apply to the personal data that was obtained from living people who are now dead. Clearly, some of the duties of the Directive do not apply. It is not possible to inform the dead person about the processing of the data or to seek their consent for new processing. However, if the data was collected from the dead person when alive for specific purposes, do duties in relation to the processing of that data continue for those stated aims? Must the processing remain lawful and fair? Must the data be kept securely? Is the effect of the death of the data subject that of removing the data from the scope of the Directive. The implementation of the Directive by Member States shows a variety of approaches to this area.

¹²¹ For issues relating uniquely to genetics – see further: *Inside Information: Balancing Interests in the Use of personal Genetic Information* (Human Genetics Commission, UK, 2002) especially at 85–7.

¹²² www.privireal.org/content/recommendations/#Recf: The PRIVIREAL project is a European Commission Framework 5 funded project examining the implementation of the Data Protection Directive 95/46/EC in relation to medical research and the role of ethics committees.

The project recommended that 'the Commission should seek to determine whether the dead are or are not to be included within the definition of "natural person" in the Directive.'

In this regard, the Article 29 Data Protection Working Party have confirmed the situation, stating that:

Information relating to dead individuals is therefore in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in civil law. However, the data of the deceased may still indirectly receive some protection in certain cases.

On the one hand, the data controller may not be in a position to ascertain whether the person to whom the data relate is still living or may be dead. Or even if he may do so, the information on the dead may be processed under the same regime as that on the living without distinction. As the data controller is subject to the data protection obligations imposed by the Directive as regards the data on living individuals, it will probably be easier for him in practice to process also the data on the dead in the way imposed by the data protection rules, rather than to separate the two sets of data.

On the other hand, the information on dead individuals may also refer to living persons. For instance, the information that the dead Gaia suffered from haemophilia indicates that her son Titius also suffers from the same disease, as it is linked to a gene contained in the X-chromosome. Thus, where the information which is data on the dead can be considered to relate at the same time also to the living and be personal data subject to the Directive, the personal data of the deceased may indirectly enjoy the protection of data protection rules.

Thirdly, information on deceased persons may be subject to specific protection granted by sets of rules other than data protection legislation, drawing the lines of what some call '*personalitas praeterita*'. The obligation of confidentiality of medical staff does not end with the death of the patient. National legislation on the right to one's own image and honour may grant also protection to the memory of the dead.¹²³

Thus, the Acts are not applicable to the dead. The protections of the Acts may arise in the case where there is joint personal data in relation to both the deceased and a living person.

Comment 1

The Acts only apply to data relating to a living person. Where data is joint personal information in relation to the dead and a living person/s, the protections may apply.

¹²³ *Opinion 4/2007 on the concept of Personal Data* at 22.

Where that is not the case then an examination of the potential position is worth considering here.

3.3 Health data for research and the dead: where the Acts do not apply

3.3.1 Professional guidelines

The UK General Medical Council states in relation to Disclosures after Death:

30. Disclosure after a patient's death

You still have an obligation to keep personal information confidential after a patient dies. The extent to which confidential information may be disclosed after a patient's death will depend on the circumstances. If the patient had asked for information to remain confidential, his or her views should be respected. Where you are unaware of any directions from the patient, you should consider requests for information taking into account:

- whether the disclosure of information may cause distress to, or be of benefit to, the patient's partner or family;
- whether disclosure of information about the patient will in effect disclose information about the patient's family or other people
- whether the information is already public knowledge or can be anonymised
- the purpose of the disclosure.

If you decide to disclose confidential information you must be prepared to explain and justify your decision.¹²⁴

The Irish Medical Council states that:

Confidentiality is a time-honoured principle of medical ethics. It extends after death and is fundamental to the doctor/patient relationship. While the concern of relatives and close friends is understandable, the doctor must not disclose information to any person without the consent of the patient, subject to paragraph 16.3.

The guidelines go on to state:

16.7 The Deceased Patient

If an insurance company requests a report on a patient who has died, the report may only be issued by the doctor of the deceased with permission from the next of kin or the executors to the estate. *The medical records of a deceased person remain confidential and death does not absolve a doctor from the obligation of confidentiality.*

¹²⁴ at Para 30. *Confidentiality: Protecting and Providing Information* (April 2004).

3.3.2 The common law

The common law perspective was examined in Chapter 1 where the courts examined what confidential information is (*Coco v. A. N. Clark (Engineers) Limited* [1969] FSR 415). We saw that the Irish courts have accepted what is regarded as confidential information (*House of Spring Gardens v. Point Blank* [1984] I.R. 611)

The court there further stated, at 664 and 696, that:

Once it is established that an obligation in confidence exists and that the information is confidential, then the person to whom it is given has a duty to act in good faith, and this means that he must use the information for the purpose for which it has been imparted, **and he cannot use it to the detriment of the informant.**

There has been some confusion over the issue of the 'detriment of the informant' criteria. This is especially so in relation to the deceased as it begs the question – what harm can come to a deceased over the release of their medical information? However, the Supreme Court, outside the medical context, has accepted this formula.

Most recently, both the UK courts and the Irish Supreme Courts have published important decisions in relation to the area of privacy and confidentiality. It should also be noted that the European Convention of Human Rights now forms part of both Irish and UK law and the rights of privacy prescribed therein cannot be ignored.

In a recent Irish decision the Supreme Court, in the case of *Mahon v. Post Publications*,¹²⁵ confirmed the nature of the duty of confidentiality, but did not comment on the issue of 'detriment'. The court, whilst approving previous authorities, stated that:

...the contours of the equitable doctrine of confidence can be described sufficiently for the purposes of this appeal, as follows:

1. The information must in fact be confidential or secret: it must... '*have the necessary quality of confidence about it*'
2. It must have been communicated by the possessor of the information in circumstances which impose an obligation of confidence or trust on the person receiving it
3. It must be wrongfully communicated by the person receiving it or by another person who is aware of the obligation of confidence.

In the House of Lords decision of *Campbell v. MGN*,¹²⁶ which related to the press disclosing

¹²⁵ [2007] IESC 15.

¹²⁶ 2 WLR [2004] 1232.

details of drug-addiction therapy being received by the model Naomi Campbell, it was stated by Baroness Hale that:

It has always been accepted that information about a person's health and treatment for ill-health is both private and confidential. This stems not only from the confidentiality of the doctor–patient relationship but from the nature of the information itself. As the European Court of Human Rights put it in *Z v. Finland* 25 EHRR 371, 405-406, para 95:

'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community.'¹²⁷

The head note of the case states the majority finding of the court:

...the threshold test as to whether information was private was to ask whether a reasonable person of ordinary sensibilities, if placed in the same situation as the subject of the disclosure, rather than its recipient, would find the disclosure offensive...¹²⁸

In this regard, Lord Hope stated that:

The mind that has to be examined is that, not of the reader in general, but of the person who is affected by the publicity. The question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity.¹²⁹

This suggests that in examining what the 'detriment' would be to the subject matter of the information (patient/deceased) the test to be used is to examine whether an objective reasonable patient/person would be offended by the disclosure.

It is to be noted, however, that the above legal authorities do not deal with the situation in relation to the deceased. As a matter of law, a person ceases to be a 'person' in the eyes of the law upon death. The question therefore arises whether that person's rights to confidentiality

¹²⁷ *ibid.*, at 1271.

¹²⁸ at 1233.

¹²⁹ at 1257.

and privacy continue after their death?

The United States courts, for example, generally accept that certain rights (such as the right to sue for defamation and the right to have 'post-mortem publicity' rights protected) lapse on death. The situation with defamation is also the case in Ireland.¹³⁰

Does a privacy interest survive death? It seems to be the case that it does not, except where disclosure of a certain type of information would cause distress to families if released. In these cases, it seems that such information has been protected from disclosure as it may affect the privacy of the existing family.

An example of this was seen in the context of Freedom of Information decisions in the US courts. For example, the press seeking release of the 'black box' tape recordings from NASA of the *Challenger* space shuttle crash which recorded the voices of the astronauts just prior to the crash. The press sought release of the tapes under freedom of information legislation stating that the tapes did not contain 'personal information' in relation to the astronauts but rather contained technical details. The court in this case in *The New York Times Company v. National Aeronautics and Space Administration* stated that:

NASA does not dispute that the substantive information contained in the tape is technical and non-personal. Rather, the 'intimate detail' that underlies the privacy interest in this tape is the sound of the astronauts' voices.... NASA... has, in fact, provided the public with a transcript of the tape's substantive contents. But how the astronauts said what they did, the very sound of the astronauts' words, does constitute a privacy interest. This is the 'intimate detail' that the Challenger families seek to protect from disclosure...The Court finds that the Challenger families' privacy interest in the tape in question outweighs the public interest such that release of the tape would constitute a clearly unwarranted invasion of the families' personal privacy.¹³¹

Similarly, in the case of *National Archives and Records v. Favish*,¹³² Favish sought investigation photographs of Vincent Foster, Jr, deputy counsel to President Clinton, deceased, who, it was claimed had committed suicide. Favish was sceptical about the government findings in this regard and wanted to see the photographs. He argued that in relation to privacy – that only extended to the individual – not to anyone else. In the context of the Freedom of Information

¹³⁰ Section 7(1) of the Civil Liability Act, 1961 states that 'On the death of a person on or after the date of the passing of this Act all causes of action (other than excepted causes of action) vested in him shall survive for the benefit of his estate.' An excepted cause of action is stated in section 6: "excepted cause of action" – means a cause of action for breach of promise to marry or for defamation or for seduction or for inducing one spouse to leave or remain apart from the other or for criminal conversation...'

¹³¹ 782 F.Supp 628 (12 December, 1991) (affirmed on appeal to the Supreme Court).

¹³² (United States Court of Appeals for the ninth circuit, 30 March 2004).

Act, the court stated that:

We disagree. The right to personal privacy is not confined...to the 'right to control information about oneself.'... To say that the concept of personal privacy must 'encompass' the individual's control of information about himself does not mean it cannot encompass other personal privacy interests as well.

...we think it proper to conclude from Congress' use of the term 'personal privacy' that it intended to permit family members to assert their own privacy rights against public intrusions long deemed impermissible under the common law and in our cultural traditions. This does not mean that the family is in the same position as the individual who is the subject of the disclosure. We have little difficulty, however, in finding in our case law and traditions the right of family members to direct and control disposition of the body of the deceased and to limit attempts to exploit pictures of the deceased family member's remains for public purposes.

The court went on to examine other cases where family privacy has been protected in connection with a family member now deceased:

In addition this well-established cultural tradition acknowledging a family's control over the body and death images of the deceased has long been recognized at common law. Indeed, this right to privacy has much deeper roots in the common law...An early decision by the New York Court of Appeals is typical:

'It is the right of privacy of the living which it is sought to enforce here. That right may in some cases be itself violated by improperly interfering with the character or memory of a deceased relative, but it is the right of the living, and not that of the dead, which is recognized. A privilege may be given the surviving relatives of a deceased person to protect his memory, but the privilege exists for the benefit of the living, to protect their feelings, and to prevent a violation of their own rights in the character and memory of the deceased.' *Schuyler v. Curtis...* (1895).

See also *Reid v. Pierce County...* (1998) ('[T]he immediate relatives of a decedent have a protectable privacy interest in the autopsy records of the deceased'); *McCambridge v. Little Rock...* (1989) (recognizing the privacy interest of the murder victim's mother in crime scene photographs); *Bazemore v. Savannah Hospital...*(1930)... (recognizing parents' right of privacy in photographs of their deceased child's body); Restatement (Second) of Torts section 652D, p. 387 (1977) (recognizing that publication of a photograph of a deceased infant – a hypothetical 'child with two heads' – over the objection of the mother would result in an 'invasion' of the mother's 'privacy').

Comment 2

Where aspects of the deceased may affect the living person by causing, especially family members, him/her harm, such connection has been recognised by the law of privacy and protected. Where private information about the deceased will affect the living individual and cause him/her harm, the public interest in disclosure will be examined and disclosure may be prohibited if harm will be caused to the living individual.

Thus, where (albeit with the context of Freedom of Information legislation) distress to the family would be caused by the release of certain types of information (in the above cases voice recordings and images of the deceased), this information will be protected from disclosure. This would however, suggest that if the family were to consent, the information could be released. In addition, the release being sought was public and in those circumstances where distress would clearly result to families, there was no public interest in the release.

3.3.3 Legislation

There is no legislation in Ireland equivalent to that in other jurisdictions. The legislation that does exist is in relation to the Freedom of Information Acts 1997–2003 (SI No. 47 of 1999 Freedom of Information Act, 1997 (section 28(6)) Regulations, 1999) – which allows certain individuals (personal representative of the deceased's estate, spouse/partner, person who has a legal function in relation to the deceased) to request and obtain personal information about a deceased person.

However, these are not of relevance here since they only operate when a party makes a request to see information, in which case the US cases above may be of some relevance. The Data Protection Acts 1988–2003, which would prohibit the processing of personal data and sensitive personal information (which medical records are) subject to certain criteria, are not applicable in relation to records of the deceased since in the Act 'personal data' is limited to data in relation to 'living individuals'. In the absence of relevant legislation, there exist only common law and ethical guidelines that might guide medical practitioners.

Thus, in looking to the examination of confidentiality at common law, one must examine:

- (i) if the information has the quality of confidence about it or is it private (i.e. something that is not in the public knowledge) – this is usually the case with medical information in a medical record
- (ii) if it was imparted in circumstances of confidence – this would be the case with information in a medical record
- (iii) that the person who was given the confidential information must use the information only for the purposes for which it was imparted (doctor, usually uses it for treatment and diagnosis unless consent has been obtained for open-end/other

uses; see discussion above in relation to access to identifiable records without consent in Chapter 2)

- (iv) if disclosure would be wrongful and to the detriment of the informant/patient (in looking at this issue of confidentiality and privacy, the UK courts seem to suggest that we look at the ordinary reasonable informant/patient to see whether such a person would find the disclosure offensive. In the case of the deceased – there is no longer a patient to make this assessment)
- (v) in addition, in the case of the deceased, would disclosure of the information cause distress to others (family members)?
- (vi) whether the individual, during their lifetime objected to post-mortem release for research? If they did, this ought to be respected.

Therefore, usually information that the medical researcher seeks access to (in identifiable format) – is confidential. No foreseeable 'detriment' can now come to the deceased from release of records in many situations, and even if it could, it would not be, generally, actionable. Whether its release would cause detriment to any interests the deceased may have or to any family members would have to be examined in every case.

One must then look to whether there is a 'public interest' exception to maintaining this confidentiality or in allowing its release and therefore access to the records. Could there be a public interest exception in the release of this information? As has been examined above, subject to recognised statutory and other public interest grounds (immediate or very high threat to public health e.g. notifiable disease), the courts have not been called upon to deal with the issue of the 'medical research public interest'.

In relation to the family/next-of-kin giving consent, this is not a situation that can in any way be compared to the organ retention issue. Certainly, in relation to a deceased adult, it does not seem that obtaining the consent retrospectively for the use of information in medical records from the next-of-kin in relation to an adult that is deceased has any argued basis in law.

It could be argued that a basis might exist if there were a direct connection in relation to the information in the medical records which is now being sought to be used – for example, where the record contains information about family members which the deceased disclosed. However, this has also been questioned by academics who have stated that:

There are difficulties with this analysis. The third party may not even be aware that the patient disclosed the information about them to the doctor. How could a duty be owed to that person in these circumstances?

They go on to state, however, that:

An alternative view would be that equity can operate upon the 'conscience' of the doctor

to protect the third party from disclosure...¹³³

Such a view may carry support. The Irish courts have indicated that the duty of confidentiality 'is essentially a moral obligation'. Thus, where a connection could be made between the information and that its release would cause distress to family members, the court might agree that this could not tally with the 'conscience' of the doctor/researcher.

The situation becomes even more difficult to consider when a medical practitioner/healthcare provider is asked by a researcher for access to the records of the deceased as in this situation, the 'consent for consent' situation obviously cannot operate. The law does not seem to have any definitive answers to these issues.

The UK Law Commission in 1981, in their report *Breach of Confidence*, opined that the estate of a deceased person could not maintain an action for a breach of confidence which caused distress to relatives if a doctor released information about the deceased (i.e. a relative cannot sue for a breach of confidence relating to a deceased). If the matter comes to be considered by the courts, it could be the case that they (through the law of equity) may insist that a doctor protect his/her patient's confidence unless there are exceptional circumstances that require that the information should be released.

As the record will not qualify as 'personal data', the protection rules of the Acts do not apply. Thus, the operation of anonymisation in this situation will be permissible. Accordingly, where possible, the consideration of anonymisation should be at the forefront of research in relation to the deceased. This will not be the desired option in all cases.

The EuroSOCAP Guide states:

The confidential nature of a patient's healthcare information and the healthcare professional's obligation to respect that confidentiality are not changed by the death of that patient. However, just as in life, the right to privacy and the duty to maintain patient confidentiality after their death are not absolute, but are subject to ethical and legal limitations.

The death of a patient never in itself permits disclosure, but it does represent a changed situation for balanced decision-making. After the death of a patient it will be more common that the balanced ethical decision will favour disclosure, as the possible harm to which the dead patient is subject is considerably reduced. The death of the patient does not automatically favour disclosure and an ethical balance must still be struck by the healthcare professional. Disclosures after death remain subject to the ethical

¹³³ Kennedy & Grubb, *Medical Law*, 3rd edn at 1083.

considerations governing any disclosure, such as whether disclosure serves a legally protected public interest and that any disclosure should be as minimal as possible.

A competent patient can give or withhold consent to disclosure before their death and such wishes should be respected as they would in other circumstances. In particular, where a competent patient has made an explicit request before his or her death that their confidence be maintained following requests from family members or carers for disclosure, then that request should normally be respected.¹³⁴

3.4 Conclusions

Medical research of the nature in question, as in most research on human subjects, should be justified in relation to its specific objectives in terms of a 'public interest' benefit.

The difficulty that may arise in some cases is that there may seem to be an almost automatic assumption that since it is the deceased whose records are being sought/obtained, then the duty of confidentiality is somehow non-existent. This is a faulty assumption.

If someone, prior to their death, directed the doctor to ensure that their file was never released for research – such a wish should be respected unless there is an overriding interest in its disclosure. Even without such a request, confidential medical information would not, in normal circumstances, be released post-mortem.

However, to suggest that this information can never be used, would clearly exclude some very important research. In the circumstances of the lack of clarity, a considered approach, such as that suggested by the UK GMC (above), may be the most sensible way forward in seeking such information.

3.5 Concluding comments

Comment 3

Notwithstanding that the proposed research pertains to the dead, research ethics committee approval must be sought.

Comment 4

A researcher should seek to ascertain whether any form of anonymisation can be utilised. If so, the data should be anonymised. If anonymisation is neither possible nor desirable, this must be explained and justified clearly to any REC.

¹³⁴ *European Standards on Confidentiality and Privacy in Healthcare* (finalised November 2005). Available at: <http://www.eurosocap.org> at 13.

Comment 5

Can the research be done in any other way or by other means? – if not – this must be explained and justified clearly to any REC.

Comment 6

Where there is no other way of doing the research (Comments 4 and 5 above), the medical records to which the researcher seeks access are going to be used for a purpose for which consent may not have ever been obtained by the now deceased. Thus, confidentiality is going to be breached unless the disclosure is justifiable on 'public interest'/'necessity' grounds. This will require detailed justification of the objectives of the research.

Comment 7

Some consideration and protection in relation to ensuring that the information is secure must be suggested.

Comment 8

The question must be asked whether there is a connection between the information and family members such that their privacy will be affected either by:

- (i) disclosing information about them or
- (ii) causing them distress.

Comment 9

To ensure that families are not 'harmed' or caused distress and that they (or the deceased if alive) would not find the disclosure offensive, researchers must consider in these circumstances, whether (i) consent from the family is possible/desirable (ii) if not (e.g. where seeking consent itself would potentially cause more harm than not seeking it), what protective measures will be taken in the research to eliminate/minimise any potential distress to family members.

Comment 10

In the absence of clear legal authority on this complex area of law, the above issues should be given careful thought by researchers, and considered and presented in detail to any REC. Researchers must always be in a position to justify the decision to use such information.

Comment 11

Thus:

- (i) medical researchers *can* access medical records of the deceased (thus, disclosure will be permissible)
- (ii) if justifiable for a specific research objective on a 'public interest' grounds and approved by an REC and
- (iii) the disclosure of this information must be 'controlled' with safeguards and measures to ensure no harm/distress is caused to families and that they or the deceased, if alive, would not find the disclosure offensive. Consideration in this regard, must also be given to potential publication of the research.

4 Implementation of the data-protection directive in Europe in relation to medical research

4.1 Introduction

Exchange of personal data between EU Member States has increased substantially with the development of the borderless internal market and the information society. In order to keep up with such developments and to protect its citizens the EU has harmonised data-protection legislation throughout its territory. To this end in 1995 the Data Protection Directive 95/46/EC ('the Directive') was enacted. This Directive in general aims to remove obstacles to the flow of personal data by requiring a high level of protection of fundamental rights (in particular, privacy) in the Member States. Each state has implemented the Directive differently and it is unclear how medical research in particular will be affected.

The Directive was implemented in Ireland in 2003. As has been examined in Chapter 2, one of the more notable features of the new law is the requirement to obtain a patient's consent before processing data, which may give rise to particular difficulties in respect of secondary or archived data.

This chapter will examine the approach to the implementation of the data-protection Directive in other Member States. It shall first deal with the exemptions to the general obligations set out in the Directive and then analyse how an exemption might be found for the purposes of medical research in Article 13.

Article 13 will be set out in full below¹³⁵ but it essentially states that Member States may restrict obligations and rights concerning the fair processing of data, information to be given to the data subject and confidentiality of data processing.

They may do so where it is necessary to safeguard for example:

- national security the prevention, investigation, detection and prosecution of:
 - criminal offences or
 - breaches of ethics for regulated professions, or
- the protection of:
 - the data subject or
 - the rights and freedoms of others.

When data are processed solely for purposes of scientific research or are kept in personal form for a period not greater than the period necessary for the sole purpose of creating statistics,

¹³⁵ See below.

Member States may restrict the data subject's right of access to data.¹³⁶

The data-protection principles provided for in Article 6(1) of the 1995 Directive are that:

Member States shall provide that personal data must be:

- (a) processed fairly and lawfully
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

4.2 Exemptions to the data-protection principles in European legislation

There are a number of exemptions or exceptions to these data-protection principles, some of which may impact upon medical research. Within each category the approach taken by the different Member States will be analysed. The exemptions are:

- Further processing for scientific purposes.
- Storage longer than necessary for scientific use.
- Processing of health data with explicit consent.
- Processing of health data of persons incapable of giving consent.
- Processing of health data for healthcare purposes.
- Processing of health data for substantial public interest
- Exemption from information to be given to the data subject.
- Exemption from the data subject's right of access to data.

¹³⁶ This is regulated by Article 12 of the Directive, which provides that a data subject has the right to confirmation as to whether or not data relating to him/her are being processed and information as to the purposes of the processing, the categories of data and the recipients to whom the data are disclosed. He/she also has the right to rectification, erasure or blocking of data, where for example they are incomplete or inaccurate.

4.2.1 Further processing for scientific purposes

The Article 6(b) principle¹³⁷ is often called the 'purpose-specification' or 'purpose-limitation' principle. There is an important exemption for scientific purposes (and therefore perhaps medical research) from this principle: processing for scientific purposes is never incompatible with any initial purpose provided that there are appropriate safeguards.

The meaning of compatible and incompatible processing

The Directive does not define incompatible or compatible processing or the means by which this should be assessed. It is therefore worthwhile examining how this provision was implemented in different countries and therefore some of its possible interpretations.

Most of the countries use the term 'incompatible' in keeping with the Directive. However, others, while alluding to the purpose principle, do not use it. For example, German law states that the storage, modification or use of personal data shall be admissible where it is necessary for the performance of the duties of the data controller and if it serves the purposes for which the data were collected.¹³⁸

These countries usually state that the data may only be further processed for the purposes for which they were originally collected. This means that where they include an exemption for scientific purposes, it has to be an exemption rather than simply a statement of incompatibility. However, in Greece there seems to be no exemptions to the purpose principle, not even for scientific purposes. It does however allow the processing of sensitive data for research and scientific purposes as a processing condition.¹³⁹

Two countries, Hungary and Lithuania, use the word 'compatible'. Neither country includes a reference to scientific research in relation to this nor therefore do the laws state that it is 'compatible' to further process data for scientific research. Bulgaria does not mention the term 'incompatible' or even allude to the purpose principle.

Only two countries, the Netherlands and Slovakia, mention 'non-incompatibility' in their respective laws. Belgium, Norway and Portugal allude to it but it is not clear whether the provisions can be interpreted more as safeguards or criteria for judgment. The Dutch law is the most explicit, stating that for the purposes of assessing whether processing is incompatible, the

¹³⁷ Member States shall provide that personal data must be:
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

¹³⁸ Section 14(1) of the Federal Data Protection Act of 20 December 1990 (as last amended 14 January 2003). The other countries are Greece, Latvia and the Czech Republic.

¹³⁹ Article 7(2)(f) of Law 2472/1997 on the Protection on Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001).

responsible party shall in any case take account of the following:

- the relationship between the purpose of the intended processing and the purpose for which the data have been obtained
- the nature of the data concerned
- the consequences of the intended processing for the data subject
- the manner in which the data have been obtained and
- the extent to which appropriate guarantees have been put in place with respect to the data subject (Article 9 (2) of the Data Protection Act 2000).

The above illustrates that there are several different means of interpreting these provisions. The first group of countries simply repeats the wording of the Directive, so there is no guidance (i.e. Austria, Cyprus, Denmark, Ireland and Spain). The second group deems a purpose to be compatible when a data subject can expect it. These countries include, for example, Sweden. The third group of countries insists that a purpose is compatible if based on a legal provision. Belgium is one example.

In Ireland an interesting approach has been taken to the definition of compatibility by the Data Protection Commissioner. He has said that he tended to take a restrictive view of the meaning of the word compatible and that he would be guided by the interpretation of the Privacy Act by the US courts. He made particular reference to *Britt v. Naval Investigative Service*¹⁴⁰ in which the court held that compatibility required a 'concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and its disclosure.'¹⁴¹ Furthermore, in Case Study No. 8 of 1999 the Irish Commissioner stated that in determining compatibility a useful test is what the data subject would reasonably have expected to happen to his or her data at the time the data was obtained.

The purpose principle and appropriate safeguards

The only safeguard provided by the Directive is that Member States must in particular rule out measures or decisions regarding any particular individual. It seems that in most countries this is not observed.¹⁴² In some cases there are no safeguards set out in the law, in some they are mentioned but not defined and in others the safeguards are highlighted and explained.

The Czech Republic provides in Article 5(4) of its 2000 Act that the data be made anonymous as

¹⁴⁰ 886 F.2d 544; 1989 US Applicant LEXIS 13826, a decision of the Court of Appeals for the Third Circuit.

¹⁴¹ Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *Implementation of the Data Protection Directive in Relation to Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005) at 181.

¹⁴² Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2004) at 210.

soon as possible, with strong security measures. In France the processing must respect the data-protection principles and procedures found in the French 2004 legislation – i.e. that data be processed fairly, lawfully and for specified, legitimate and explicit purposes. In Norway the public interest in the research must prevail over the potential disadvantages, while in Malta Article 8 of the Data Protection Act 2002 states that appropriate safeguards must be put in place when the data are kept for longer periods and the data must not be used for decisions relating to an individual. In the UK (similarly to Ireland) it states that *the data must not be processed to support measures or decisions in relation to the individual and it must not cause damage or distress to any data subject* (author's emphasis).

Other countries also have safeguards in relation to this principle and medical research.¹⁴³ Those countries with a purpose principle, an exemption for science, and no safeguards in the law appear to be Belgium, Finland, Italy, Slovakia and Spain. This position is not compliant with the Directive, which states that the scientific purpose *can only* be viewed as not incompatible with the initial purposes *provided* that the country furnish appropriate safeguards.¹⁴⁴

The fact that the Directive is not specific in relation to what types of safeguards must be provided causes differences throughout the whole of Europe and problems for every type of pan-European business. Some safeguards must be provided and those countries that do not provide them do not properly implement the Directive.¹⁴⁵

Belgium

The relevant Belgian law¹⁴⁶ states that 'under the terms established by the King ... further processing of data for scientific purposes shall not be considered incompatible.' Neither of the terms 'further processing' nor 'scientific purposes' have been defined. In the report to the King however, it is specified that scientific research also means population research with a view to protecting and promoting public health. It would seem therefore that scientific research is understood in a broad sense. According to the same report, further processing means that the individual responsible wishes to re-use the data for scientific purposes himself or that he communicates them to another. The Royal Decree also provides for the following safeguards:

Anonymisation Article 3 states that the further processing has to be performed in principle on anonymous data that are not personal data any longer i.e. their processing does not require any specific guarantees to be given to the data subject.

¹⁴³ i.e. Austria, Germany (which includes many safeguards) Latvia, Luxembourg, the Netherlands, Poland, Portugal and Sweden.

¹⁴⁴ Beyleveld *et al.* as above, fn 143 at 211.

¹⁴⁵ Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005) at 212.

¹⁴⁶ Data protection is covered by the Law of 8 December 1992 on Privacy Protection as modified by the law of 11 December 1998 and by Royal Decree of 13 February 2001.

Coding of Data. If it is not possible to use anonymous data, the researcher must determine whether it can be done with coded data. If so, there is a number of safeguards. The data must be coded before further processing for scientific purposes takes place. If the further processing relates to sensitive data (including health data) before coding takes place, the data subject must be informed of the scientific purpose of the further processing, the origin of the data, his right to access and correction and his right to oppose the further processing (Art. 14). Article 15 gives an exemption to this obligation to inform the data subject, based on Article 11(2) of the Directive.

Non-coded Data. This is strictly regulated in section 3 of the Royal Decree. There is no distinction between health data and other types of sensitive data. The data subject must receive precise information on the scientific purposes of the further processing and he must give express consent. It is interesting to note that for practical considerations the Directive does not require written consent but only adequate safeguards. Article 20 lays down the possibility of an exemption from the obligations to inform the data subject (and implicitly the obligation to obtain consent) based on Article 11(2) of the Directive.

Denmark

The Act on Processing of Personal Data states that the collection of data shall take place for specified, explicit and legitimate purposes and they shall not be further processed in a way incompatible with these purposes. Further processing of data exclusively for scientific purposes shall not be considered incompatible with the purposes for which the data were collected.

Norway

The Norwegian Act of 14 April 2000 Relating to the Processing of Personal Data provides that the controller shall ensure that personal data which are processed are not used subsequently for purposes that are incompatible with the original purpose of the collection without the consent of the data subject. Therefore, the subsequent processing of personal data for scientific purposes is not incompatible with the original purposes, if the public interest in the processing being carried out clearly outweighs the possible disadvantages for natural persons.

The Netherlands

The Personal Data Protection Act 2000 provides in Article 9(1) that personal data shall not be processed in a way incompatible with the purposes for which they have been obtained. Subsection 2 outlines a series of factors to evaluate whether further processing is incompatible with these purposes. Further processing for historical, statistical or scientific purposes shall not be regarded as incompatible where the responsible party has made the necessary arrangements to ensure that further processing is carried out solely for these purposes. The explanatory memorandum explains that necessary arrangements can mean measures of a legal nature such as a code of conduct, a convention, written agreements but also technical or

organisational provisions. The legislature attempted to draw a distinction between pure scientific research (allowing further processing) and commercially funded research. However, the Directive makes no such distinction.

4.2.2 Storage longer than necessary for scientific use

According to the fifth data-protection principle,¹⁴⁷ Member States shall provide that personal data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or further processed. This is so even if later uses cannot be predicted. This requirement clashes with research needs for retaining personal data for many years. For example, the extensive studies of several decades' worth of data on the effects of oral contraceptives, and of oestrogen replacement therapy, would not have been possible had this constraint been in place at the time of these studies' inception.¹⁴⁸ However, the Article goes on to provide that Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

As has been noted,¹⁴⁹ this is of particular importance for the secondary use of medical data for research purposes. Research on data initially collected for other purposes can have many varied and important contributions to health. A substantial amount of research is carried out electronically through databases and includes for example aspects of epidemiology, public-health surveillance, studies of patterns of occurrence, determinants and natural history of disease and evaluation of healthcare interventions and services.

Belgium

Article 4, section 1(5°)¹⁵⁰ provides that appropriate safeguards must be laid down for personal data that are stored for a longer period than necessary for scientific purposes. However, the legislation does not define or elaborate on what these safeguards are. It merely states that safeguards will be laid down by the king after taking advice from the Commission for the Protection of Privacy, which is the national supervisory authority.

Denmark

Article 5(5) states that the data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which data are processed.

¹⁴⁷ Article 6(1)(e) of Directive 95/46/EC.

¹⁴⁸ See Lowrance W, *New Laws in Europe*, Privacy and Health Research (1997) 2, available at: <http://aspe.os.dhhs.gov/datacncl/PHR5.htm>

¹⁴⁹ Beyleveld D, Townend D, Rouillé-Mirza D, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005) at 52.

¹⁵⁰ The Law of 8 December 1992 on Privacy Protection as modified by the Law of 11 December 1998 and by Royal Decree of 13 February 2001.

Norway

According to Article 28, the controller shall not store personal data for longer than is necessary to carry out the purpose of the processing. However, the controller may store personal data for scientific purposes if the public interest in the data being stored clearly prevails over the disadvantages for the persons concerned. In this case, the controller shall ensure that the data are not stored for longer than necessary in ways which make it possible to identify that data subject.

The Netherlands

Article 10(2) provides that personal data may be kept for longer than necessary for achieving the purposes for which they were collected or subsequently processed. This is where this is for scientific purposes and where the responsible party has made the necessary arrangements to ensure that the data concerned are used solely for these specific purposes. Again necessary arrangements have not been defined in the legislation.

4.2.3 Processing of health data with explicit consent

Article 8(1) of the Directive asserts that Member States must prohibit the processing of personal data concerning health. However, Article 8(2)(a) goes on to provide that this prohibition is not applicable where the data subject has given his/her explicit consent to the processing of such data.

As Nys has noted¹⁵¹ while this article envisages some scope for the processing of personal health data for research purposes, some researchers consider it problematic. They argue that it is too difficult, expensive and time consuming to seek a patient's consent. It may also be difficult to ascertain whether a patient actually is able and willing to consent and furthermore may lead to selective non-response, thus lessening the value of research.¹⁵²

Belgium

Article 7 section 1 prohibits the processing of health related personal data. But this prohibition does not apply if the data subject has given his/her written consent, on the understanding that the consent can be withdrawn at any stage. In such a case the Royal Decree stipulates that there must be prior communication of the reasons for the processing by the data controller. This goes further than the Directive, which requires just explicit consent.

Article 27 of the Royal Decree states that even with the written consent of the data subject, where the latter is in a dependent position towards the individual responsible, the prohibition on processing of sensitive personal data continues to apply. However, there is an exception to this

¹⁵¹ See fn no. 186, at 52–3.

¹⁵² See also Callens, 'The privacy directive and the use of medical data for research purposes' (1995) 2 *European Journal of Health Law* 309.

where the processing confers a benefit on the data subject. The most common example of this type of situation is the employer–employee relationship.

Here the employer cannot process sensitive personal data based on the employee's written consent, unless there is an advantage granted to him or her, such as the payment of union subscription fees, benefits or where the employer wants to grant his employees of any particular religion certain specific facilities.

Denmark

According to Article 7(1) no processing of personal data concerning health may take place. But this provision does not apply where the data subject has given his/her explicit consent to the processing of such data.

According to Article 35(1) a data subject may at any time object to the processing of data relating to him/her. Where justified, the processing can no longer involve those data. The data subject can also withdraw his/her consent.

Norway

Sensitive personal data (defined as information relating to health) may be processed only if one of a number of conditions is satisfied *and* the data subject consents to the processing. Among these conditions are the protection of the vital interest of the data subject and the performance of a task in the public interest.

Mere consent is all that is required; it does not have to be explicit or written. Consent is defined in Article 2(7) as a free, specific and informed declaration by the data subject. Furthermore, consent on its own is not a sufficient condition to process health data.¹⁵³

If the data subject gives consent, the principle of confidentiality will cease to apply to the extent of the consent given. Even if the data subject has consented, the controller must decide on the basis of his/her opinion on what is best for the patient and if he/she is in a condition to be able to consent.

The Netherlands

Article 16 prohibits the processing of personal data concerning a person's health, but not where this is carried out with the explicit consent of the data subject (Article 23(1)).

¹⁵³ Note however that Engelschion seems to imply that consent is a sufficient condition: 'Health data may however only be processed if the processing also satisfied one of the conditions set out in Article 9 in the personal data act. If the processing is based on consent or statutory authority, the section has no independent position. If the processing is based on the six mentioned exceptions in Article 8, section 9 sets up *additional requirements* (emphasis added).' (Engelschion S, "The Implementation of Directive 95/46 in Norway, especially with regard to medical data" (2002) 9 *European Journal of Health Law* 192.

Article 23(2) also provides for an exemption to the explicit consent rule for the purposes of scientific research.

However, even where the data subject has given explicit consent to the processing of health data, for example, his/her consent to communicating his/her health data to a researcher, it may be prohibited for the person responsible, i.e. the treating physician, to do so. Article 9(4) states that a person's data cannot be processed where there is a duty of confidentiality by virtue of office, profession or legal provision. According to one view,¹⁵⁴ this means that the processing of health data is prohibited when medical professional secrecy so demands. Such secrecy can act as a 'correction' to the general processing data-protection rules. In this way criminal, disciplinary and civil regulations for medical confidentiality are incorporated in general data-protection law.

Article 21(4) contains a very strict provision for the processing of genetic data. It states that:

personal data concerning inherited characteristics may only be processed, where this processing takes place with respect to the data subject from whom the data concerned have been obtained, unless:

- a. a serious medical interest prevails or
- b. the processing is necessary for the purposes of scientific research or statistics.

This may mean that even with the consent of the data subject, genetic data may not be processed with respect to any person, other than the data subject him or herself, except in (a) and (b) above.¹⁵⁵

4.2.4 Processing of health data of persons incapable of giving consent

Researchers point out that the explicit consent rule would prevent any research using the data of a person unable to give explicit consent, such as children and the disabled. Here Article 8(2)(c) comes into play and provides that the prohibition of processing health data does not apply if it is necessary to protect the vital interest of the data subject or of another person. The scope of this article is not however, very clear.

In Ireland this exemption is covered by section 2A (1)(a) of the 2003 Act. It holds that where the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it may be given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject where the giving of such consent is not prohibited by law.

¹⁵⁴ Hooghiemstra T, 'The implementation of Directive 95/46/EC in the Netherlands with special regard to medical data' (2002) 9 *European Journal of Health Law* 225.

¹⁵⁵ *ibid.*

4.2.5 Processing of health data for healthcare purposes

Article 8(3) of the Directive states that the prohibition on processing health data does not apply where the processing is required for:

- the purposes of preventative medicine
- medical diagnosis
- the provision of care or treatment or
- the management of healthcare services.

This is where the data are processed by a health professional subject to the obligation of professional secrecy under national law or rules established by national competent bodies, or where they are processed by another person, also subject to an equivalent obligation of secrecy.

As this provision does not mention processing for the purpose of medical research, a question arises as to whether it is covered by 'preventative medicine' and 'medical diagnosis' and whether it allows for an exemption to the explicit consent rule. The position is not very clear. If it is covered, this might permit the processing of sensitive data for the purposes of medical research. This question is of particular importance since medical researchers must at some stage process health or genetic data and perhaps other sensitive data. If this provision does not apply to medical research, it would mean that researchers would have to either anonymise the sensitive data, inform the data subject or stop processing the data to carry out the research. On the contrary, if the provision does include medical research, it would mean that the processing of sensitive data would be lawful so long as the controller respects the other provisions of the data-protection Directive.¹⁵⁶

It should also be noted that the Directive does not define medical research; it therefore throws little light on the topic. It can be understood broadly and taken to mean the use of medical (health) data for epidemiology, pharmacovigilance and clinical trials. It may be understood as scientific research, comprising both pure scientific research and applied scientific research (i.e. the use of scientific methods without aiming at the creation of new knowledge).¹⁵⁷

Only three of the EU countries considered that 'preventative medicine' and 'medical diagnosis' cover medical research. But four seem to exempt the processing of sensitive data for the purpose of medical research. In Ireland section 2B of the 2003 Act and the UK 1998 Act lifted the prohibition of processing sensitive data in the case of processing for medical purposes. Medical purposes include medical research, medical diagnosis and preventive medicine.

¹⁵⁶ Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005) at 212

¹⁵⁷ As above, at 51.

Luxembourg exempts processing made for a purpose of medical diagnosis, preventive medicine and scientific research in biological and medical fields. In Sweden it is said that the prohibition of processing of sensitive data does not apply when:

Processing is required for purpose of medical diagnosis, preventive medicine, [...] or where those data are processed by a health professional subject...¹⁵⁸

This means that in Sweden processing of sensitive data can be undertaken for medical research, with the only condition being that health professionals do it. This seems to be less strict than the Directive. This is because the latter imposes two conditions:

- that the processing is made by a health professional
- *and* for a purpose of medical diagnosis or preventive medicine.

Yet the Swedish law uses 'or' instead of 'and'. Moreover, section 19 allows the processing of sensitive data for research and statistics purposes, provided the interest of society in the project is manifestly greater than the risk of violation of the data subject's personal integrity. This would seem to be a liberal approach to the processing of sensitive data for medical research in comparison with other countries in Europe.¹⁵⁹

In other countries, processing for medical research could be exempted provided it is considered as processing for scientific purposes, or for the purpose of medical diagnosis or preventive medicine. In Finland, for example, the law does not have a provision similar to Article 8(3) of the Directive. Section 12 of the Act contains two exemptions to the prohibition of processing of sensitive data: (i) an exemption for processing for historical, scientific or statistical research and (ii) for processing for healthcare purposes. The former could include medical research, depending on the interpretation given to the provision. In this case the Finnish law would clearly allow the processing of sensitive data for medical research even without the data subject's consent.

In Belgium, Article 7 of the Data Protection Act 1998 mirrors the Directive and does not mention medical research. However, under Belgian law processing sensitive data for scientific research is acceptable, but only under conditions established by the King after advice from the Commission for the Protection of Privacy. In Denmark, the law also repeats the Directive and it seems that medical research is encompassed by the provision only if it is undertaken for preventive medicine or medical diagnosis. If not, another provision of the Danish law applies.

Finally in some of the countries the provisions concerning medical research are independent

¹⁵⁸ Section 18, Act of 29 April 1998.

¹⁵⁹ Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005) at 213.

from those concerning medical diagnosis and preventive medicine. In Spain and Norway under the interpretation of the laws given in the domestic reports, medical research would not seem to be included under medical diagnosis and preventive medicine. France and Germany seem to apply specific conditions to the processing of sensitive data for medical research and do not consider that art 8(3) of the Directive covers the case of medical research.

In France, the 2004 Act merely repeats the provision in the Directive. However, Article 40 of the French 1978 Data Protection Act is retained in the legislation. This article concerns the processing of personal data for research in the health sector, which is allowed under specific conditions. One of these is that the results of the research cannot be disclosed if they enable identification of the data subjects.¹⁶⁰ The Act adds that when the research uses biological samples enabling identification of the data subject, the prior and express consent of the data subject must be obtained. This would seem to show that processing for medical research does not have the same rules as processing for medical diagnosis or preventive medicine. The processing of sensitive data for those purposes is allowed without the consent of the data subject, which is not the case for medical research.¹⁶¹

Belgium

Article 7, section 2(j) echoes the Directive and states that the prohibition of processing health data is not applicable if necessary for the purposes of preventative medicine or medical diagnosis, the provision of care or treatment to the data subject or to one of his/her relatives, or the management of healthcare services operating in the interest of the data subject and only if those data are processed under the supervision of a health professional.

According to some,¹⁶² explicit consent is not required when Article 7, section 2(j) is applied. They contend that in all these cases the therapeutic relationship between a patient and a health professional is at stake. However, this is not the case when health data are processed not for the treatment of the data subject him or herself but for the treatment of one of his/her relatives. This provision is not in accordance with the Directive. It could potentially clear the way for non-consensual processing of health data that is not directly in the interest of the data subject, such as medical research.

Norway

Article 9(g) states that health data may be processed if one of the conditions set out in Article 8 is satisfied and the processing is necessary for the purposes of preventative medicine, etc. and where the data are processed by health professionals subject to the obligation of professional secrecy.

¹⁶⁰ Article 40 (4) of the Law 78–17 of 6 January 1978 on Informatics and Freedoms.

¹⁶¹ Beyleveld D *et al.* above fn 161, at 213.

¹⁶² Boulanger, Callens and Brillon, 'La protection des données à caractère personnel'(2000–2001) *Rev. Dr. Santé* 334.

The Netherlands

According to Article 21(1)(a) the prohibition on processing personal data concerning a person's health does not apply where the processing is carried out by medical professionals, healthcare institutions or facilities or social services provided that this is necessary for the proper treatment and care of the data subject or for the administration of the institution or professional practice concerned.

In the Dutch literature no indications can be found that this provision also applies to medical research.¹⁶³

4.2.6 Processing of health data for substantial public interest

The Directive provides different exemptions in Article 8 to the prohibition of processing of sensitive data but none of them directly refer to processing carried out for medical research.

Article 8 reads as follows:

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:
 - (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
 - (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
 - (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
 - (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
 - (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

¹⁶³ Beyleveld D *et al.* as above, fn 161, at 61.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 8(3) of the Directive does not seem to have been interpreted very often by the Member States as applying to medical research, with the result that often an exemption to the sensitive processing conditions could instead be interpreted as stemming from the public interest requirements in subsection 4.

Recital 34 of the Directive cites public health and scientific research as areas where important reasons of public interest may justify derogation from the ban on processing of health data. Member States do not have a free rein in enacting rules to communicate medical data for research purposes without the data subject's cooperation, as this would be a violation of Article 8 of the European Convention on Human Rights. (Article 8 deals with the right to respect for private and family life.)¹⁶⁴ It is arguable that any such rules would be contrary to the principle

¹⁶⁴

Article 8

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.

of necessity contained therein.¹⁶⁵ This principle means that in a democratic society interference with the exercise of an individual's right must be necessary for one or more of the purposes specified in Article 8(2).

At issue in Article 8(4) of the Directive is whether Member States interpret medical research to be in the public interest (see Chapter 2). While on the one hand it is difficult to assume that all medical research is in the public interest and benefits more people than it disadvantages, it very much depends on the type of research. The substantial public interest in research on major infectious diseases such as avian influenza and SARS is clear for example.

The majority of countries implement Article 8(4) by repeating the Directive's wording, but without expanding upon the definition of 'substantial public interest'. In certain countries, however, the respective provisions contain references which could be interpreted as including medical research. In Luxembourg, the Data Protection Act states that the prohibition does not apply where the processing is necessary for reasons of public interest, especially for historical, statistical or scientific purposes. The Act adds that, in such a case, the Supervisory Authority should give its prior authorisation to the processing. If it interprets medical research as being of public interest and having a scientific purpose, then it could authorise the processing of sensitive data.

Norway and Sweden have enacted similar provisions. Processing necessary for scientific research where the public interest clearly exceeds the disadvantages or risks it might entail for the data subject could be exempted from the prohibition on processing sensitive data. In the UK the secretary of state is empowered to remove the prohibition on processing sensitive data.¹⁶⁶ The Data Protection (Processing of Sensitive Personal Data) Order 2000¹⁶⁷ states that the prohibition is removed where processing is necessary for research purposes that are in the substantial public interest. No examples are given by the Order.

It has been seen above that certain countries have not directly used the exemption for substantial public interest to exempt processing of sensitive data made for medical research. However, it is arguable that a particular interpretation of the implementing domestic laws could lead to an exemption of such processing. It can therefore be said that authorising the processing of sensitive data for medical research because of its substantial public interest is a real possibility.

¹⁶⁵ Beyleveld D *et al.* fn 143 at 325.

¹⁶⁶ Schedule 3, Para. 10 of the Data Protection Act 1998.

¹⁶⁷ SI 417/2000.

Belgium

Protection and promotion of public health

Article 7, section 2(d) implements Article 8(4) of the Directive and states that there is no prohibition if processing is necessary for the protection and promotion of public health. This includes population screening. It would appear that no suitable safeguards have been provided for by national law.

Scientific research

Article 7, section 2(k) states that the prohibition is not applicable if processing is necessary for scientific research and carried out under certain conditions.¹⁶⁸ The Royal Decree was necessary in order to fulfil the requirement of Article 8(4) of the Directive that 'suitable safeguards' must be provided for. However, the Royal Decree only applies to *further* processing of health data for scientific purposes. It does not contain any provision regarding the *primary* processing of health data for scientific purposes. Member States may provide for an exemption by either national law or by the supervisory authority. However, the Belgian Supervisory Authority has no decision making competence, rendering this exemption next to useless.

Denmark

Processing for reasons of substantial public interest

Article 7(7) permits exemptions where it happens for the above reason. The supervisory authority shall give its authority in such cases and the processing may be made subject to specific conditions. The supervisory authority shall notify the commission of any derogation.

Processing for scientific studies of significant social importance

Health data may be processed for this reason under Article 10(1), where it is necessary in order to carry out these studies. The data cannot be subsequently processed for anything other than statistical or scientific purposes and can only be disclosed to a third party with the supervisory authority's leave. The authority is empowered to lay down detailed conditions concerning the disclosure.

Suitable safeguards

The following are some examples of the 'suitable safeguards' Member States use in relation to scientific research and the implementation of Article 8(4) of the Directive.¹⁶⁹ Safeguards are not always mentioned in domestic laws in the context of the exemption for the public interest, but it

¹⁶⁸ These conditions were established by the king in a decree agreed upon in the Council of Ministers after advice from the Commission for the Protection of Privacy.

¹⁶⁹ Article 8(4) states that subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down additional exemptions either by national law or by decision of the supervisory authority.

is worth mentioning them as examples of how the concept of safeguards has been understood by the Member States.

Norway

For scientific purposes with important public interests

Article 9(h) allows health data to be processed if one of the conditions set out in Article 8 is satisfied, the processing is necessary for scientific purposes and the public interest in such processing being carried out clearly surpasses the disadvantages it might entail for the natural person. The necessity requirement is quite strict and implies that the processing must be necessary without the consent from the individual.¹⁷⁰

For important public interests

The last sentence of Article 9 states that the Data Inspectorate may decide that sensitive personal data may also be processed in other cases if this is warranted by important public interests and steps are taken to protect the interests of the data subject.

In Austria there are strict rules and in some cases a permit is required from the supervisory authority for the processing of sensitive data for scientific research and statistics.¹⁷¹ In Cyprus all measures taken must be for the protection of the data subject.¹⁷² In Germany the advantages of the research project must trump the data subject's interest in opposing collection *and* the research purpose must not be achieved by other means without unreasonable effort.¹⁷³ In Greece anonymity is recommended for processing in scientific research *and* all processing of sensitive data must gain a permit. The lack of specification in Sweden as to what type of safeguard to use may actually be helpful as, depending on the substantial public interest, the country can decide what type of safeguard is relevant in the particular context. However, this flexibility could also make it difficult for an international medical research organisation to follow correctly and accurately the different requirements of the law in each country, thus perhaps causing a barrier to said research.¹⁷⁴

All other countries surveyed for this section also included safeguards to the substantial public interest provision, where it was included in their law.¹⁷⁵

¹⁷⁰ Engelschion S at fn 156 above, at 193.

¹⁷¹ Pursuant to ss 9(1)(10) and 46 of the *Datenschutzgesetz* 2000.

¹⁷² Article 6(2)(h) of the Law on the Processing of Personal Data (Protection of Individuals). Law 138 (I) 2001.

¹⁷³ s.13(2)(8) Federal Data Protection Act 20 December 1990 as amended most recently on 14 January 2003.

¹⁷⁴ Beyleveld D *et al.* fn 161 above, at 219.

¹⁷⁵ Belgium, Denmark, Estonia, Finland, Hungary, Ireland, Malta, the Netherlands, Norway, Portugal, Romania and the UK.

The Netherlands

An important public interest

As per Article 23(1)(e), the prohibition on processing data concerning a person's health does not apply where this is necessary having regard to an important public interest, and where appropriate guarantees have been put in place to protect individual privacy. It must also be provided by law or an exemption must have been granted by the Data Protection Commission. When so doing, the Commission can impose rules and restrictions. Furthermore, such processing must be notified to the European Commission.

For scientific research serving a public interest

Article 23(2) of the Dutch law excludes the prohibition where:

- the research serves a public interest
- the processing is necessary for the research concerned
- it appears to be impossible or would involve a disproportionate effort to ask for express consent, and
- sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent

This article has a broad field of application. It applies not only when health data are collected primarily with a scientific purpose but also in the case of further processing for scientific purposes but which was originally processed for other purposes and/or stored longer.

As regards the third condition (exemption from asking express consent), Hooghiemstra states that the patient has influence in relation to the use of medical data for research purposes in so far as it would involve a proportionate effort for the researcher to ask for express consent. The general rule in the data-protection law does not even give the patient the right to object.¹⁷⁶ However, in addition to the general rule, the Dutch have specific regulations with regard to the communication of health data by the treating physician to researchers (further processing). These can be found in Articles 457 and 458 of the Medical Treatment Contracts Act (also called the Patient's Rights Act).¹⁷⁷

There are also detailed rules laid down by the research community and published in a Code of Conduct for Health Research. This distinguishes between the uses of non-identifiable data, identifiable but coded data and other identifiable data. The code has been approved by the Data Protection Authority.

¹⁷⁶ Beyleveld D *et al.* as above, fn 161, at 224.

¹⁷⁷ Article 457 stipulates that medical data may only be communicated to a researcher with a patient's consent. Article 458 outlines two exceptions: (i) communication of personal data is allowed provided that the research is carried out without unreasonably violating the patient's right to privacy; (ii) encoded data can be communicated without consent if asking the patient is not possible in view of the nature and purpose of research.

For the purpose of scientific research with genetic data

Article 21(4) asserts that genetic data (i.e. data concerning inherited characteristics) may only be processed where this takes place with respect to the data subject from whom the data concerned have been taken. Even with the explicit consent of the data subject, processing of such data with respect to another person is prohibited unless necessary for the purposes of scientific research. Express consent is required. However, Article 21(4)(b) refers to Article 23(2) which means that if all conditions of this article are fulfilled then an exemption from the explicit consent is possible. The data subject has no right to object.

4.2.7 Exemption from information to be given to the data subject

Where data have not been obtained from the data subject (e.g. a medical researcher receives the subject's medical data from the treating physician), Article 11 (1) obliges the Member States to provide that the data subject is given the information mentioned in that sub-article i.e.:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing;
- (c) any further information such as
 - the categories of data concerned,
 - the recipients or categories of recipients,
 - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

However, Article 11(2) of the Directive negates this obligation to inform where, in particular for the processing for the purposes of scientific research, the provision of such information proves impossible or would involve a disproportionate effort. There is also no obligation to inform if recording or disclosure is expressly laid down by law. In these cases, the Member States must provide appropriate safeguards. As indicated by Recital 40 of the Directive the number of data subjects, the age of the data and any compensatory measures may be taken into consideration in this respect.

It appears that 14 countries ¹⁷⁸ provide in their domestic law that the right to information does not apply when processing is undertaken for the purpose of scientific research or for a scientific purpose. However, not all of these provide this exemption exclusively when data are not obtained from the data subject. Some countries do not make any distinction between the case of Articles 10 and 11 of the Directive. In the Netherlands, even if Article 11(2) is implemented in

¹⁷⁸ Austria, Belgium, Cyprus, the Czech Republic, Germany, Ireland, Latvia, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania and Spain

domestic law; the Medical Treatment Contracts Act states that medical data are particularly protected and that an informed consent (involving information to be provided to the data subject) must be obtained from the data subject before the disclosure of such data outside a medical team.

France provides an exemption to the right to information in the case of storage of the data for historical, statistical or scientific purposes when data have been collected for another purpose. There is also an exemption where the provision of information proves impossible or would involve a disproportionate effort. Thus the French information is slightly different to the provisions of the Directive by adding an exemption (case of storage) to the right to information in the case of processing for scientific purposes. In Portugal, certain disclosures of personal data must be made by force of law even without informing the data subject, for example in the cases of declaration of infectious and contagious diseases and communication of health expenses to the social security system.

Several of the other countries do not mention the case of scientific research as a case where the exemption applies, but in general these countries have implemented Article 11(2) by mentioning that the exemption applies where the provision of information proves impossible or would involve a disproportionate effort, without specifying that this is specifically the case for processing for scientific research.¹⁷⁹ In Finland the exemption seems to apply to registries made with patients' records from public healthcare. In the UK it is said in the 1998 Act that the Secretary of State could create an exemption for data processing related to the physical or mental health condition of the data subjects¹⁸⁰. Finally, in Denmark an interpretation of the *travaux préparatoires* suggests that there is only a very limited obligation to inform the data subject when the data have been collected for scientific purposes.

In conclusion, it would appear that the Article 11(2) exemption has been implemented by a large majority of the European countries. It is difficult to assert conclusively that this means therefore that the data subject must be informed in all cases of processing for scientific purposes. However, a certain disparity can be seen between countries that outline particular situations in which the exemption to the right to information applies, especially relating to the processing of medical data or medical research, and other countries where the exemption provided in Article 11(2) is not mentioned clearly¹⁸¹.

¹⁷⁹ Denmark, Finland, Italy, Lithuania, Norway and the UK

¹⁸⁰ Section 30, Data Protection Act, 1998.

¹⁸¹ Beyleveld D *et al.* fn 161 above, at 221–2.

Belgium

Further processing of health data for scientific purposes

When health data are further processed in a coded form for scientific purposes, the data subject must be informed of the scientific purposes. As already noted above 'scientific purposes' has not been defined in the Belgian legislation. However, this obligation does not need to be respected if the provision of such information proves impossible or would involve disproportionate effort and provided the procedure contained in Article 16 has been followed. This requires that additional information has to be communicated to the Commission for the Protection of Privacy. This commission must rule on the request not to inform the data subject within 45 days (which period can be prolonged for another 45 days). If the commission has not communicated a recommendation after this period has expired, the request is considered to be accepted.

When health data are further processed in a non-coded form, the informed consent of the data subject is required. However, similarly to the Article 16 procedure outlined above, if this proves impossible or would involve disproportionate effort, such consent is not necessitated.

Denmark

Article 29(3) states that information is not required to be provided to the data subject where it is impossible or would involve disproportionate effort. In addition, it does not need to be provided if the data subject's interest in obtaining this information is found to be overridden by vital private interests, including his/her own.

Norway

Under Article 20 a controller who collects personal data from persons other than the data subject must inform the data subject of which data are being collected and provide such information as:

- the name and address of the controller and of his/her representative, if any
- the purpose of the processing
- whether the data will be disclosed and if so, the identity of the recipient
- the fact that the provision of data is voluntary and
- any other circumstances that will enable the data subject to exercise his/her rights in the best possible way, such as information on the right to demand access to data¹⁸², and the right to demand that data be rectified¹⁸³ as soon as the data have been obtained.

¹⁸² Cf. section s.18

¹⁸³ Cf. sections 27 and 28.

However, there is an exemption to the requirement to give information to the data subject if:

- (a) the collection or communication of data is expressly authorised by statute
- (b) notification is impossible or disproportionately difficult or
- (c) there is no doubt that the data subject already has the information which shall be contained in the notification.

The Netherlands

The requirement to give information to a data subject where data has not been obtained from him/her does not apply, if it seems impossible or would involve disproportionate effort. However, in the case of further processing for scientific purposes, a different article, Article 44(1), becomes the pertinent one. Article 44 provides that where processing is carried out by institutions or services for the purposes of scientific research, and the necessary arrangements have been made to ensure that the personal data can only be used for scientific purposes, the responsible party is not required to provide the information referred to in Article 34.

4.2.8 Exemption from the data subject's right of access to data

Article 12 obliges Member States to guarantee every data subject the right of access to data relating to him or her. According to Article 13(2) Member States may derogate from Article 12 where:

- data are processed solely for the purposes of scientific research or
- kept in personal form for a period that does not exceed the period necessary for the sole purpose of creating statistics

provided that:

- the restriction is by a legislative measure
- there is clearly no risk of breaching the privacy of the data subject and
- adequate legal standards are provided, in particular that the data are not used to take measures or decisions regarding any particular individual.

Belgium

According to Article 10, section 2 any person has the right to gain knowledge of the personal data that are processed relating to his/her health whether directly or with the assistance of a health professional. If there is no risk of violating the privacy of the data subject and if the data are not used for taking measures and decisions with regard to him or her, communication may be postponed if the health-related data are processed for purposes of medical scientific research. This is only to the extent that communication would interfere seriously with the research and only postponed until no later than the moment at which the research has ended. In that case, the data subject must have given in advance his/her explicit consent to the controller both to the personal data being processed for purposes of medical scientific research

and to the communication of the personal data relating to him/her being postponed.

According to the explanatory report to this article this exemption from the right of access to data is necessary in order not to make double-blind clinical trials impossible by having to tell a patient to what group he/she belongs. This article requires explicit consent but in the light of Article 8(2) it should be read as a written consent.

Denmark

Article 2(1) of the Danish Data Protection Act provides that any rules on the processing of personal data in other legislation, which give the data subject better legal protection, shall take precedence over the rules laid down in this Act. Nys questions whether the duty to medical professional secrecy constitutes a 'rule' of the processing of personal data and whether it provides a better legal protection.¹⁸⁴

Under Article 2(2) the Act shall not apply where this will be in violation of the freedom of information and expression in Article 10 of the ECHR.¹⁸⁵

Norway

There is no right of access if the personal data are being processed exclusively for scientific purposes and the processing will have no direct significance for the data subject. Moreover, the right of access and the obligation to provide information do not apply, where it would be regarded as inadvisable for the data subject to gain knowledge of such information or data. This is out of consideration for the health of the person concerned or for the relationship to persons close to the person concerned.

The Netherlands

Article 44 holds that there is no requirement to accede to a data subject's request as to whether personal data are being processed, where the processing is being carried out by institutions or services for the purposes of scientific research and the necessary arrangements have been made to ensure that personal data can only be used for scientific purposes.

¹⁸⁴ Nys H in Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds.) *The Data Protection Directive and Medical Research Across Europe* (Aldershot,: Ashgate Publishing Ltd, 2005) at 67

¹⁸⁵ Article 10

1 Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

4.3 Article 13 and exemptions in relation to medical research

This section considers Article 13 and:

- firstly exemptions to the data-protection principles generally (i.e. that data must be processed fairly, lawfully and for specified, explicit and legitimate purposes: see Article 6 of the 1995 Directive) and
- secondly the right to information and the right of access in relation to medical research generally.

Article 13 reads:

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

The main question to be considered here is how far Article 13(1) of the Directive can be and has been applied to exempt medical research from the data-protection principles. In order for Article 13(1) to exempt medical research one of following categories of data would need to be invoked:

- (a) national security
- (b) defence

- (c) public security
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e)
- (g) the protection of the data subject or of the rights and freedoms of others.

The most obvious category which might be employed to exempt medical research is Article 13(1)(g) i.e. the protection of the data subject or the rights and freedoms of others. However, in addition one commentator argues that for example:

...there might be cases where medical research to develop biological weapons or, more plausibly, to defend against them, could be necessary for (a) to (c). Provision (d) could be appealed to in relation to the investigation of fraud in medical research. Medical research is also, arguably, an important economic or financial interest of the Member States...¹⁸⁶

It now seems apposite to survey Member States to ascertain whether medical research had already been directly interpreted as an exemption falling directly under the Article 13(1)(g).

Using the exemption to Article 6(1)

Article 6(1) of the Directive outlines the data-protection principles. These include the requirement that data be processed fairly and lawfully.

Only 10 of the 27 countries surveyed have an exemption from the data-protection principles relating to conditions (a) to (g) set out in Article 13(1). Eight of these include such exemptions by exempting from the whole of the relevant act.¹⁸⁷ In a few instances, it is stated in the Acts that the exempted categories are, in fact, regulated by other Acts.¹⁸⁸ Five countries included direct exemptions from the data-protection principles. These are the Czech Republic, Ireland, Malta, Netherlands, and the UK.

Exemptions to the Data Protection Principles for Medical or Scientific Research

As previously noted above, possibly the only means of including medical or scientific research

¹⁸⁶ Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd. 2005) at 73.

¹⁸⁷ Denmark, Estonia, Ireland, Latvia, Lithuania, Malta, The Netherlands and Romania.

¹⁸⁸ For example, Latvia in relation to state secrets and the Netherlands which includes many examples

under the 13(1) exemptions might be to define it as the protection of the data subject or the rights and freedoms of others. Three countries appear to include an exemption: Malta, The Netherlands and the UK.

Malta

Malta includes an exemption to the data-protection principles in section 23(1)(g) of its Act¹⁸⁹ for processing where information is prejudicial to the protection of the data subject or to the rights and freedoms of others.

The Netherlands

There is an exemption to the incompatibility principle to protect the rights and freedoms of others. Article 9 states that personal data shall not be further processed in a way incompatible with the purposes for which they have been obtained. In assessing whether processing is incompatible, the responsible party should take into account:

- (a) the relationship between the purpose of the intended processing and the purpose for which the data have been obtained
- (b) the nature of the data concerned
- (c) the consequences of the intended processing for the data subject
- (d) the manner in which the data have been obtained, and
- (e) the extent to which appropriate guarantees have been put in place with respect to the data subject.

It goes on to add that the further processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible where the responsible party has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes.

Article 43, however, states that Article 9(1) does not apply where this is necessary in the interests of protecting the rights and freedoms of others.

The UK

Processing for health, education and social work can be exempted from the first data-protection principle (as far as it requires compliance with information provisions) by the Secretary of State. The Secretary of State can make further areas exempt from all or part of the first data-protection principle's provisions that he/she considers necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual.

¹⁸⁹ The Data Protection Act of 22 March 2002

Exemptions to the rights to information using Article 13(1) and medical research

Compared to restrictions to the data-protection principles, restrictions to the rights to information (and the controller's duty to provide it) are reasonably common. Some include an exemption to the whole of the implementing law for categories such as national security, state secrets, defence, or criminal law within the scope of said laws. Sometimes within these laws there are often even more limits placed on the right to information. There is already an exemption from the Article 11 information provisions for processing for scientific research in Article 11(2).¹⁹⁰

There are eight countries which provide the opportunity for exempting from the information provisions for the protection of the data subject or the rights and freedoms of others.¹⁹¹ Other countries include an exemption to both information provisions for other related issues. See for example the UK's exemptions in relation to health, education and social work, which could possibly relate to medical research.

Czech Republic

There are exemptions from both the information provisions for information processed exclusively for scientific purposes under Article 11(5)(a) of the Act.¹⁹² It is possible to assume that in this case this interpretation is brought directly from the Article 13 provision for protecting the rights and freedoms of others and that medical research would be included as a scientific purpose. However, it is also possible that it is a wide interpretation of Article 11(2) of the Directive even though there is no mention of disproportionate effort.¹⁹³

France

There is an exemption to both rights of information if, for legitimate reasons, the physician is of the opinion that the patient should not be informed of a severe diagnosis or prognosis.

Luxembourg

There are exemptions from both information provisions for scientific research.¹⁹⁴ However, there are also provisions dealing with circumstances where it is impossible to notify or this

¹⁹⁰ This states that where providing information to the data subject is impossible or would require a disproportionate effort, and appropriate safeguards are observed, the data controller or his/her representative would not have to provide any information

¹⁹¹ Denmark, Estonia, Hungary, Luxembourg, Malta, the Netherlands, Norway and Slovenia.

¹⁹² Act on the Protection of Personal Data (4 April 2000).

¹⁹³ Beyleveld D *et al.* fn 161, as above, at 203

¹⁹⁴ Article 27(3) of the Law on the Protection of Persons with Regard to the Processing of Personal Data (2 August 2002).

involves a disproportionate effort and therefore this is probably an expansive interpretation of the Directive's Article 11(2) provisions.

The Netherlands

Scientific research is exempt from provision of information when not obtained from the data subject, with no clause for impossibility or disproportionate effort (Article 44 of the Dutch legislation). This could be seen either to be related to the Article 13 exemptions for the protection of rights and freedoms of others or a broad interpretation of Article 11(2).

Norway

Includes an exemption to the information provisions where it is inadvisable for the data subject to gain such knowledge out of consideration for the health of the person concerned or for the relationships with persons close to him/her.¹⁹⁵ This may be relevant to medical research only perhaps where it is for the benefit of a relative. There is another noteworthy exemption where it would be contrary to obvious and fundamental private or public interests to provide such information. If medical research may be viewed as a public interest, then this could apply.

Portugal

There are waivers from both information provisions for processing for scientific research where there is a legal provision or a decision of the supervisory authority under Article 10(5)-(6).¹⁹⁶ However, as there are provisions on when it is impossible to notify or involves a disproportionate effort, this might also be read as a wide interpretation of the Directive's 11(2) provisions.

The UK

There are exemptions in section 30(1) of the Data Protection Act to both information provisions for 'personal data consisting of information as to the physical or mental health or condition of the data subject' when provided for by the Secretary of State.

Exemptions to the Right of Access using Article 13 for Medical Research

Article 12 of the Directive includes a provision that the data subject has the right to:

- receive confirmation as to whether data are being processed about him/her
- ask for the logic behind automatic decisions
- to request rectification, erasure or blocking when the data are incomplete or inaccurate.

¹⁹⁵ Section 23(c), Personal Data Act, 14 April 2000

¹⁹⁶ Act on the Protection of Personal Data, 26 October 1998.

The data controller must also notify these changes to third parties, unless it is impossible to do so.

Article 13(2) of the Directive also provides an exemption when data are processed solely for scientific research or statistics, under certain conditions. In the implementing laws the right of access is often included as a separate provision from the right to rectification and notification to third parties. Ten countries provide exemptions to the right of access to protect the rights and freedoms of others.¹⁹⁷

Bulgaria

There is a restriction on the right of access for cases which relate to national health in Article 27 of the data-protection Act. This could relate to medical research where it is will benefit national health.

Denmark

There is an exemption to the right of access for scientific purposes but it is silent as to the risk of breaching the privacy of the data subject and to the fact that the processing will not be used to take measures relating to the individual. It seems therefore that this exemption is not an implementation of Article 13(2).¹⁹⁸

Finland

There is an exemption from the rights of access when providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else.¹⁹⁹ In addition, section 27(1)(3) exempts data if it used solely for scientific research.

Italy

There is exemption from the right of access and rectification by legislative decree if the outcome significantly affects the outcome of the research.

Norway

Includes an interesting exemption to the right of access where it is inadvisable for the data subject to gain such knowledge out of consideration for the health of the person concerned.

Poland

There is an exemption from right of access for scientific purposes if it involves disproportionate effort.

¹⁹⁷ These are Bulgaria, Estonia, Finland, Hungary, Luxembourg, Malta, the Netherlands, Norway, Slovenia and Spain.

¹⁹⁸ Beyleveld D *et al.* fn 161 above at 205.

¹⁹⁹ Section 27(1)(2) of the Personal Data Act.

Spain

This Spanish exemption²⁰⁰ states that the rights of access and rectification do not apply when superseded by reasons of public interest or the interests of third parties more worthy of protection. There is also a separate exemption for the protection of the rights and liberties of third parties in Article 23(1) of the Spanish law. This exemption also includes as safeguards firstly that a reasoned justification should be provided to the supervisory authority and secondly that the data subject should be informed of his/her right to appeal to the authority. Medical research could conceivably be encompassed by both 'public interest' and the interests of third parties more worthy of protection.

The Netherlands

Scientific research is exempt from the right of access, with the only stipulation being that the controller ensures that the data will be used only for these purposes.

The UK

The right of access is exempted in relation to health if the Secretary of State so orders. Research purposes are also exempt from the section 7 right of access, as long as the results of the research are not in a form which would identify the data subjects.

4.4 Conclusions

It has been shown that there are a number of exemptions to the data-protection requirements outlined above which could relate to medical research and that these have been implemented in many different ways across the EU.

It has been seen for example that Member States differ in relation to how they define incompatible processing. Furthermore, while some provide safeguards, many do not. The fact that neither 'incompatibility' nor 'safeguards' have been defined or clarified by the Directive causes differences throughout Europe. Those countries that do not provide safeguards of any kind have not, it must be suggested, implemented the directive properly. It is of particular importance that Member States provide and detail adequate safeguards, because if adequate safeguards are provided, it facilitates the secondary use of medical data for research purposes. Although the Directive prohibits the processing of personal health data, it is not applicable where the data subject has given his/her explicit consent. Again, the diverging positions of the countries have become obvious. One Member State, Belgium, has a stricter requirement than that envisaged by the Directive, while in Norway the consent does not, for example, have to be written.

Where data processing is required for the purposes of preventative medicine, medical diagnosis

²⁰⁰ Article 24(2) of the Law on the Protection of Personal Data, 13 December 1999.

or the provision of care or treatment, the diverse positions of the Member States can be seen. As noted, only a minority (of which Ireland is one) have taken a 'liberal' approach. In addition, using the 'substantial public interest' exemption would seem to provide a possibility for exemption for medical research. The exemption from information to be given to the data subject seems to have been implemented by the majority of Member States.

In relation to Article 13 and medical research we have seen that three countries have availed of what may be the only means of including medical or scientific research under the exemption in subsection 1 i.e. they have defined it as the protection of the data subject or of the rights and freedoms of others. Some Member States are exempt from the information provisions for these reasons.

As directives are binding only as to the result to be achieved, permitting the Member States to choose the form and methods that they will use for implementing the directive, this affords them some flexibility in fashioning their legislation to deal with their individual concerns, especially in relation to medical research. However, even given the latitude afforded to the Member States, the position in relation to medical research remains ambiguous. This is because flexibility can only go so far. The exemptions to the data-protection principles exist for a reason and cannot be used to enable data controllers to circumvent their obligations under the directive.

4.5 Concluding comments

Comment 1

Whatever direction is taken in the future, consistency of approach would be advisable and important lessons ought to be learnt from the Member States and from other jurisdictions. This wide wisdom of experience can only serve to benefit and improve Ireland's approach to data-protection in the sphere of medical research.²⁰¹

²⁰¹ For the situation in relation to other countries e.g., the US, which regulates the issue of privacy by way of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), see further for a detailed account: Annas GJ. 'HIPAA regulations — a new era of medical-record privacy?' 348 *New England Journal of Medicine* 2003: 1486–90, where the author concludes that 'The implementation of the new HIPAA privacy regulations is likely to be costly, inconsistent, and frustrating to both physicians and patients. Medical privacy is critical to most Americans, national privacy standards would be welcome, and the promise of privacy remains essential for much medical treatment.'

5. Bibliography

5.1 Articles, books, guidelines and reports

Academy of Medical Sciences (2006) *Personal Data for Public Good: Using Health Information in Medical Research*, Academy of Medical Sciences, UK.

Adams T. *et al* (2004). 'Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent', 328 *BMJ* 871–4.

Al-Shahi R & Warlow C (2000) Using patient-identifiable data for observational research and audit. *BMJ*, 321:1031–2.

Annas GJ (2003) 'HIPAA regulations — a new era of medical-record privacy?' *New England Journal of Medicine* 348:1486–90.

Australian Code for the Responsible Conduct of Research (2007) Jointly issued by the National Health and Medical Research Council, the Australian Research Council and Universities Australia.

Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *The Data Protection Directive and Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2004).

Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds) *Implementation of the Data Protection Directive in Relation to Medical Research Across Europe* (Aldershot, Ashgate Publishing Ltd, 2005).

BMA Guidance on Secondary Uses of Patient Information (2007) Ethics Department, British Medical Association, UK.

BMA Consent Toolkit (2003) 2nd edn February at:
<http://www.bma.org.uk/ap.nsf/Content/consenttk2~card2>

Boulanger, Callens and Brillon, 'La protection des données à caractère personnel' (2000–2001) *Rev. Dr. Santé* 334.

Callens, 'The privacy directive and the use of medical data for research purposes' (1995) 2 *European Journal of Health Law* 309.

Canadian Institutes of Health Research (2005) Best Practices for Protecting Privacy in Health Research, Public Works and Government Services Canada.

Casabona CMR (2005) 'Anonymization and pseudonymization: the legal framework at a European level'. In: Beyleveld D, Townend S, Rouillé-Mirza S, Wright J. *The Data Protection Directive and Medical Research Across Europe* (Ashgate, Aldergate Ltd. UK).

Canadian Institutes for Health (2002) *Secondary Use of Personal Information in Health Research: Case Studies*. Public Works and Government Services Canada.

Case P (2003) The rise and fall of informational autonomy in medical law. *Med. L. Rev.*, 11(2):208.

Council for International Organizations of Medical Sciences (2002) International Ethical Guidelines for Biomedical Research Involving Human Subjects.

Cousins G. *et al.* (2005) *Public Perceptions of Biomedical Research – A survey of the general population in Ireland*. Royal College of Surgeons of Ireland with the Health Research Board and

the Department of Health and Children.

Data Protection Guidelines on Research in the Health Sector (Data Protection Commissioner, Dublin, 2007).

Department of Health and Children (1999) *Children First*, Ireland.

Delany H (2005) 'Breach of confidence or breach of privacy: the way forward'. *Dublin University Law Journal*, 25:151.

Engelschion S (2002) 'The Implementation of Directive 95/46 in Norway, especially with regard to Medical Data' 9 *European Journal of Health Law* 192

European Standards on Confidentiality and Privacy in Healthcare (finalised November 2005). Available at: <http://www.eurosocap.org>

General Medical Council (2004) *Confidentiality: Protecting and Providing Information*. (GMC, UK).

Gillot J (2006) *Human Rights, Privacy and Medical Research: Analysing UK Policy on Tissue and Data*. Genetic Interest Group, UK.

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

Health Information and Quality Authority (HIQA) (2006/2007) *Annual Report of the Interim Health Information and Quality Authority* (HIQA, Ireland).

Hooghiemstra T. (2002) 'The Implementation of Directive 95/46/EC in the Netherlands with Special Regard to Medical Data' 9 *European Journal of Health Law* 225.

Human Genetics Commission (2002) *Inside Information: Balancing Interests in the Use of personal Genetic Information*. Human Genetics Commission, UK.

Irish Medical Council (2004) *A Guide to Ethical Conduct and Behaviour*. 6th edn, Irish Medical Council, Dublin.

IMS Health (2002) *European Commission Review of EU Data Protection Directive 95/46/EC (IMS Health)* (available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/paper/imshealth_en.pdf).

Irish College of General Practitioners (2003) *Managing and Protecting the Privacy and Personal Health Information in Irish General Practice: An Information Guide to the Data Protection Acts for General Practitioners*. The Irish College of General Practitioners and the National General Practice Information Technology Group, Dublin.

Irish Council for Bioethics (2005) *Human Biological Material: Recommendations for Collection, Use and Storage in Research* (Irish Council for Bioethics, Dublin).

Irish Council for Bioethics (2004) *Operational Procedures for Research Ethics Committees: Guidance* (Irish Council for Bioethics, Dublin).

Jackson E (2006) *Medical Law: Text, Cases and Materials*. Oxford University Press, UK.

Kennedy I and Grubb A (2000) *Medical Law*. 3rd edn, (Butterworths, UK).

- Lachmann PJ (2003) Consent and confidentiality – where are the limits? An introduction. *J. Med. Ethics*, 29:2–3.
- Laurie G. (2002) *Genetic Privacy: A Challenge to Medico-legal Norms* (Cambridge University Press, UK).
- Lennon P (2005) *Protecting Personal Health Information in Ireland: Law & Practice*. (Oak Tree Press, Ireland).
- Lowrance W (2002) *Learning from Experience: Privacy and the Secondary Use of Data in Health Research*. (Nuffield Trust, UK).
- Madden D and McDonagh M (2004) Implementation of Directive 95/46/EC in relation to Medical Research in the Republic of Ireland. In: Beyleveld *et al.* (eds) *Implementation of the Data Protection Directive in relation to medical research in Europe* (Ashgate, UK).
- Mason JK and Laurie GT (2006) *Mason & McCall Smith's Law and Medical Ethics*. 7th edn, (Oxford University Press, UK).
- Medical Research Council (MRC) (2000) *Personal Information in Medical Research*, (MRC, UK).
- Metcalf *et al.* (2008) 'Low risk research using routinely collected identifiable health information without informed consent: encounters with the Patient Information Advisory Group'. *J. Med. Ethics*, 34:37–40.
- McDonagh M. (2006) *Freedom of Information Law*. 2nd edn, (Thomson, Ireland).
- McMahon B and Binchy W (2000) *Law of Torts*. 3rd edn, (Butterworths, Dublin).
- National Statement on Ethical Conduct in Human Research*. Developed jointly by National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, 2007.
- Nys H. 'The Scope of Exemptions in medical research' in: Beyleveld D, Townend S, Rouillé-Mirza S, Wright J (eds.) (2005) *The Data Protection Directive and Medical Research Across Europe* (Aldershot: Ashgate Publishing Ltd. UK).
- O'Neill O (2003) Some limits of informed consent. *J. Med Ethics*, 29:4–7.
- Peto J. et al. "Data Protection, informed consent, and Research" *BMJ*, 2004;328:1029-30.
- Phillipson G (2003) Transforming Breach of Confidence? Towards a common law Right of Privacy under the Human Rights Act. *Modern Law Review*, 66:726–32.
- Sheikh AA (2007) Lessons for healthcare from litigation: 2007 – a busy time for medical law. *Medico-Legal Journal of Ireland*, 13(2):54–62.
- Sheikh AA (2005) The Data Protection (Amendment) Act, 2003: The Data Protection Directive and its implications for medical research in Ireland. *Eur. J. Health Law*, 12:357.
- Sheikh AA (2002) *Genetic Research and Human Biological Samples: The Legal and Ethical Considerations*. Health Research Board: www.hrb.ie
- Strobl J. Cave E, Walley T. 'Data Protection legislation: Interpretation and barriers to research' *BMJ*, 2000; 321:890-892
- The Confidentiality & Security Advisory Group for Scotland (2002) *Protecting Patient Confidentiality* (CSAGS, Scotland) available at: <http://www.show.scot.nhs.uk/csags/>

The Medical Council (2004) *Guide to Ethical Conduct and Behaviour*. 6th edn, (The Medical Council, Dublin).

Turnberg L (2003) Common sense and common consent in communicable disease surveillance' *J. Med. Ethics*, 29:27–9.

UK Department of Health (2001) *Building the Information Core: Protecting and Using Confidential Patient Information, A Strategy for the NHS*. (Information Policy Unit, UK).

UK Information Commissioner (2002) *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998* (Information Commissioner, UK).

UK Law Commission (1981) *Breach of Confidence*. (Cmnd 8388, HMSO, London).

5.2 Cases

Canada

- *Allan v. Mount Sinai Hospital* 28 O.R (2d) 356.

European Court of Human Rights

- *MS v. Sweden* Reports 1997-IV 1437, (1999) 28 EHRR 313.
- *Z v. Finland* (1998) 25 EHRR 371.

Ireland

- *EH v. Information Commissioner* (No. 2) [2002] 3 IR 600.
- *Fitzpatrick v. Eye and Ear Hospital* (Unrep. SC., 15 Nov. 2007), Kearns J.
- *House of Spring Gardens v. Point Blank* [1984] IR 611.
- *In re a Ward of Court* [1996] 2 IR 79.
- *Kennedy v. Ireland* [1987] 1 IR 587.
- *Mahon v. Post Publications* [2007] IESC 15.
- *McGrory v. ESB* [2003] 3 IR 407.
- *M. R. v. T. R., Walsh & Ors* [2006] IEHC 359.
- *National Irish Bank v. RTE* [1998] 2 IR 465.

United Kingdom

- *AB v. CD* (1851) 14 D 177.
- *Campbell v. MGN Ltd* [2004] 2 AC 457, 2 WLR [2004] 1232.
- *Chester v. Afshar* [2005] (HL) 1 AC 134.
- *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.
- *Hunter v. Mann* [1974] QB 767 at 772.
- *R v. Department of Health, ex parte Source Informatics Ltd* [2000] 1 All ER 786.
- *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd* (1948) RPC 203 at 211.
- *W v. Egdeell* [1990] Ch (CA) 359 at 419.

United States

- *National Archives and Records v. Favish*, United States Court of Appeals for the ninth circuit, 30 March 2004.
- *Tarasoff v. Regents of the University of California* (1976) 131 Cal Rptr 14 (Cal Sup Ct).
- *The New York Times Company v. National Aeronautics and Space Administration* 782 F.Supp 628 (12 December, 1991) (affirmed on appeal to the Supreme Court).

5.3 Legislation, law, ethical policies, recommendations, opinions

Ireland

- The Irish Constitution, 1937 (as amended).
- Health Act, 1947.
- Civil Liability Act, 1961.
- Road Traffic Act, 1961.
- SI 105/1971, the Health Services Regulations, 1971.
- Data Protection Acts, 1988 and 2003.
- Child Care Act, 1991.
- Statistics Act, 1993.
- Road Traffic Act, 1994.
- Freedom of Information Act 1997 and 2003.
- Social Welfare Act, 1998 (as amended).
- (SI No. 47 of 1999 Freedom of Information Act, 1997 (section 28(6)) Regulations, 1999).
- European Convention on Human Rights Act, 2003.
- SI No. 190 of 2004, European Communities (Clinical Trials on Medicinal Products for Human Use) Regulations 2004.
- Disability Act, 2005.
- SI No. 305 of 2007, The Health Research Board (Establishment) (Amendment) (No.3) Order, 2007.

Europe

- 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 (Official Journal 1995 L 281).

Sweden

- Swedish Personal Data Act (1998: 204).

United Kingdom

- Data Protection Act, 1998.

International

- Universal Declaration of Human Rights, 1948.
- European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.
- Council of Europe 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, 1997.
- Declaration of Geneva World Medical Association, revised 2000.
- Charter of Fundamental Rights of the European Union, 2000.
- Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, 2005.
- International Code of Medical Ethics, World Medical Association, revised 2006.
- Recommendation No. R (97) 5 *On the Protection of Medical Data* Committee of Ministers, 13 February, 1997.
- *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998*, UK Information Commissioner, May 2002.
- *Data Protection Guidelines on Research in the Health Sector* Data Protection Commissioner, Dublin, 2007.
- Data Protection Working Party. *Opinion 4/2007 on the Concept of Personal Data*, 20 June 2007.