Canadian Institutes of Health Research | Instituts de recherche en santé du Canada

Canada

Selected International Legal Norms on the Protection of Personal Information in Health Research

CIHR IRSC
Canadian Institutes of Health Research | Instituts de recherche en santé du Canada

December 2001

Canadian Institutes of Health Research
410 Laurier Avenue West
Ottawa, Ontario K1A 0W9
www.cihr.ca

Cat. No. MR21–31/2001E–IN
ISBN 0–662–31428–X

Canadian Institutes of Health Research | Instituts de recherche en santé du Canada

Canada

Selected International Legal Norms on the Protection of Personal Information in Health Research

December 2001

Overview of Document

(Detailed Table of Contents follows.)

Detailed Table of Contents

List of Abbreviations Used in this Report

BMA	British Medical Association
CCPR	*International Covenant on Civil and Political Rights*
CESC	*International Covenant on Economic, Social and Cultural Rights*
CIHR	Canadian Institutes of Health Research
CNIL	National Data Processing and Liberties Commission (Commission nationale de l'informatique et des libertés de la France)
COE	Council of Europe
COE Convention 108/1981	*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*
COE Convention on Human Rights and Biomedicine	*Convention for the Protection of Human Rights and the Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*
COE Recommendation R97(5)	*Recommendation on the Protection of Medical Data*
DPA	*Data Protection Act*
ECHR	*European Convention on Human Rights*
EEC	European Economic Community
EU	European Union
EU Charter	*European Union Charter of Fundamental Rights*
EU Privacy Directive	EU *Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*
European Group on Ethics Opinion	*Ethical Issues of Healthcare in the Information Society, Opinion No. 13*
FAQs	Frequently Asked Questions
HHS	US Department of Health and Human Services

HIPAA Privacy Rule	Standards for Privacy of Individually Identifiable Health Information
HIPAA	*Health Insurance Portability and Accountability Act*
HIPC	*Health Information Privacy Code*
HREC	Human Research Ethics Committee
IPPs	The Public Sector Standards: Information Privacy Principles (part of the *Privacy Act* of Australia)
Joint NHMRC/AVCC Statement	Joint NHMRC/AVCC Statement and Guidelines on Research Practice
Law 78-17	*Law 78-17 Respecting Data Processing, Records and Freedoms* (*Loi n^o 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*)
Law Respecting Archives	*Loi n^o 78-18 du janvier 1979 relative aux archives*
Medical Treatment Contract Act	*Wet geneeskundige behandelingsovereenkomst*
MRC	Medical Research Council (UK)
MRC Guidelines	*Medical Research Council Guidelines on Research and Personal Data*
NHMRC	National Health and Medical Research Council (Australia)
NPPs	*The Private Sector: National Privacy Principles* (part of the *Privacy Act* of Australia)
OECD	Organization for Economic Co-operation and Development
OECD Guidelines	*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*
PDPA	*Personal Data Protection Act* (*Wet bescherming persoonsgegevens*)
PIPED	*Personal Information Protection and Electronic Documents Act*
RHIR	*Retention of Health Information Regulations* (1996)
UK	United Kingdom

UN	United Nations
UN Guidelines	*Guidelines for the Regulation of Computerized Personal Data Files*
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNESCO Declaration	*Universal Declaration on the Human Genome and Human Rights*
Universal Declaration	*Universal Declaration of Human Rights*
US	United States
WHO Declaration	*Declaration on the Promotion of Patients' Rights in Europe*
WHO	World Health Organization
WMA	World Medical Association
WWII	World War II

Executive Summary

In April 2000, the Canadian Institutes of Health Research (CIHR) published *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research.* The compendium was prepared as part of a broader attempt to inform the current debate over how to respect peoples' right to have their personal information protected while also allowing health researchers reasonable access to such information in order to better the health of Canadians, improve health services and strengthen the Canadian health system.

This new document supplements the 2000 *Compendium* with an overview of international standards that protect personal information. This international perspective situates Canada's position in a global context. Canvassing how other jurisdictions are addressing this debate, and identifying trends in privacy legislation, can provide models for Canada to emulate or avoid as we prepare to address the challenging issues that lie ahead.

For instance, the increasing pace of international collaborative health research, the revolution in information and communication technologies between nations, and new transnational privacy laws are globalizing both scientific research and international privacy standards. Some of these international standards affect Canadian governmental norms and public policy. New laws, both federal and provincial, are emerging. As Canadian society moves toward the development and refinement of such laws, an understanding of how we correspond to and differ from other nations can help us choose personal information standards for Canada.

This survey is selective, not exhaustive. Part II outlines the establishment of human privacy as a principle of international law in tandem with the development of related human rights and ethical norms during the post-World War II era (1945–1970). The standards sampled include those from the *Nuremberg Trials* (1947), the *Universal Declaration of Human Rights* (1948), the *European Convention on Human Rights* (1950), the *International Covenant on Civil and Political Rights* and *International Covenant on Economic, Social and Cultural Rights* (1960s and 1970s), and the World Medical Association's *Declaration of Geneva* (1948) and *Declaration of Helsinki* (1964, 1975 and 2000). The fundamental principles of privacy, confidentiality and consent share a common purpose: the promotion and protection of human dignity. When applied, however, these rights and duties sometimes give rise to quandaries. Some of the human rights instruments of the post-WWII era provide standards that can help deal with the tension between important public values and can help refine tests for balancing privacy with other societal needs. They recommend an explicit "necessity" test to justify infringements of privacy in accordance with the law in order to advance such pressing democratic needs as public safety or the protection of health.

Part III of this document outlines modern international data protection principles and laws that began to be developed. Drawing on the international privacy standards from 1945 to the 1970s, these principles and laws go on to define specific and detailed norms for balancing the right to privacy with legitimate societal uses of personal information. The standards sampled include those of the Organization for Economic Co-operation and Development (OECD), the Council of Europe (COE), the European Union (EU), and the United Nations (UN). Each of these has exerted particular international influence.

The 1980 principles of the OECD laid the foundations for minimizing obstacles to the free flow of data across borders while ensuring respect for the right to privacy. They have influenced subsequent international and national documents on data protection, and have guided the deliberations, policies and laws of some 30 member states of the OECD.

The Council of Europe has an equally long history of data protection initiatives within Europe. It has adopted a general data protection convention and defined standards for medical information. The UN adopted a variation of the OECD principles in 1990. It added norms on consent, confidentiality, and data protection in UNESCO's 1997 *Universal Declaration on the Human Genome and Human Rights*. Perhaps most influential within recent years has been the 1995 *Privacy Directive* of the EU. The Directive aims at harmonizing standards by obliging the EU's 15 member states to ensure that national legislation conforms to the Directive. Because it is binding, detailed and generally prevents the exchange of data with nations lacking "adequate" privacy protections, the Directive has helped reform data protection and privacy laws across Europe, in Australia, the United States (US) and Canada.

Part IV of this report profiles selected national data protection laws: those of Australia, France, the Netherlands, New Zealand, the United Kingdom (UK) and the US. Like Canada, most of these nations have recently reformed national data protection statutes that initially incorporated or reflected the original OECD principles. Australia recently amended its federal *Privacy Act* with new standards for the private sector, consistent with revised norms for publicly funded health research. Its neighbour, New Zealand, has a similar *Privacy Act*. It authorizes the Privacy Commissioner to develop sectoral codes of conduct, like the recently revised *Health Information Privacy Code* of 1994. The UK, too, has recently updated its former data protection law to conform to the *EU Privacy Directive*. The Medical Research Council and the British Medical Association have complemented the revised UK data protection law with detailed guidelines on the use of personal information for medical research. Legislation to revise the French central data protection law is before the French Parliament, though France amended its law in 1994 with specific provisions to govern health research. Similarly, the Netherlands has already enacted a new data protection law. This section also looks at US laws, including the *Federal Privacy Act* of 1974, the new federal regulations on the protection of health information, and the recent US response to the *EU Privacy Directive*.

To ease comparison, this report profiles these national laws and international standards according to these aspects: (a) the scope of the law; (b) relevant definitions; (c) special protections for sensitive data; (d) consent requirements for data collection, use and disclosure; (e) general exceptions allowing non-consensual processing of data with particular focus on research; (f) aspects regarding data retention and security; and (g) other noteworthy provisions.

This comparative analysis of international norms underscores trends and issues relevant to the development and refinement of Canadian standards for processing personal information in the health research context. For example, the data protection laws of countries such as the UK, Australia and the US, as well as those in the EU, define such terms as "identifiable" personal information, "consent," and "research." Some of the jurisdictions canvassed also define health information as a class of sensitive data that warrants special protections and standards. Consent remains the general requirement for the processing of such information.

In exceptional circumstances, laws and standards authorize the non-consensual processing of personal information in certain circumstances in order to advance other pressing societal needs. Such circumstances, in many cases, expressly include statistical or scientific research. The exact conditions that justify the exception depend on the nation's law. Generally, such processing of identifiable personal information must be shown to be necessary for the purposes of the research, individual consent must be objectively impracticable to obtain, adequate security safeguards must be implemented to protect the confidentiality of the data subject(s), and data processing must be restricted to the minimum necessary in terms of scope, duration and retention. Laws in countries such as Australia and New Zealand have also expressly coordinated public processes between the Federal Privacy Commission and Ministry of Health in order to develop detailed health sector norms and codes of conduct consistent with federal privacy law.

I. Introduction

This document is a companion to the Canadian Institutes of Health Research (CIHR) publication *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research* (April 2000).[1] In the process of concluding that compendium, CIHR was inspired by certain important trends and developments to profile international standards on the protection of personal information.

The increasing pace of international collaborative health research, the revolution in information and communication technologies across nations, and new transnational privacy laws are globalizing both scientific research and international privacy standards. Some of those international standards inevitably affect Canadian governmental norms and public policy. Canada has not only an interest but a role and responsibility in setting the course for these international trends.

Moreover, in concert with such evolving international developments, the Government of Canada has recently enacted new federal privacy standards in the *Personal Information Protection and Electronic Documents Act*[2] (PIPED Act); provinces and territories are likely to follow suit with substantially similar legislation. As Canadian society moves toward the refinement of such laws, an understanding of how we correspond to and differ from other nations may lead to more effective implementation of personal information standards. Such standards affect government, universities, researchers, health information holders/users, policy analysts and the public.

This document examines established and emerging personal health information standards and approaches in the international community—some parallel those in Canada and some differ. The study focuses on comparative international legal standards, such as federal privacy, data protection, and confidentiality laws. Selected ethical, professional and governmental norms are also identified because of their influence on national and international public policy. This compendium is selective rather than comprehensive; even within particular jurisdictions the analysis is selective, in order to profile instructive examples.

Part I of this international compendium provides a brief overview. Parts II and III turn to the international community to examine standards, largely those of international governmental entities such as the United Nations (UN), Organization for Economic Co-operation and Development (OECD), European Union (EU) and Council of Europe (COE). Such standards are outlined in historic and new legal instruments, as well as in public policy and ethics declarations. Part IV profiles selected national approaches in Australia, France, the United Kingdom (UK), the Netherlands, New Zealand and the United States (US).

---

1 Public Works and Government Services Canada. *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research.* Ottawa: Public Works and Government Services Canada, 2000.

2 *Personal Information Protection and Electronic Documents Act*, S.C. 2000. c.5. Online: http://www.privcom.gc.ca/

To facilitate the comparative analysis, each jurisdiction is profiled on the basis of the following questions:

a. *Scope of the Law:* Does the law or policy apply to the public sector, private sector or particular organizations?

b. *Definitions*: How are terms such as “personal information,” “health information,” “data processing” and “consent” defined, if at all? (Note that within this report, the term “data processing” generally refers to the collection, use and disclosure of data. However, the guidelines and laws in various nations may define “data processing” in ways that parallel or differ from this meaning.)

c. *Special Protections: Sensitive Data*: Is health information subjected to general personal information standards or is it subject to special provisions?

d. *Consent: Data Collection, Use and Disclosure*: What standards govern consent to the collection, use or disclosure of personal and health information?

e. *Exceptions and Research:* Are there specific exceptions for collection/use/disclosure of personal information for research purposes?

f. *Data Retention and Security*: Do standards specify processes for safeguarding data**,** time limits for its retention, or requirements for the destruction of data?

g. *Other Noteworthy Provisions*: Does the law or policy outline other notable, innovative or instructive provisions?

It should be noted that the research for this document is generally current to May 2001.

II. Post-WWII International Privacy Principles (1945 to the 1970s)

This section outlines the development and evolution of privacy principles, largely under international human rights law, in the immediate aftermath of World War II (WWII). Many of the initial and enduring international legal standards on privacy were crafted during this era. These helped to lay the foundation on which modern international data protection laws and principles now stand.

A. The Broader Heritage of Nuremberg: Human Dignity, Consent and Privacy in Research

The emergence of privacy as a fundamental principle of modern international human rights law resulted, in part, from the community of nations' response to the excesses, atrocities and abuses committed during World War II. In 1945, the international community responded by creating the United Nations, with its commitment to "the dignity and worth of the human person" and respect for and observance of fundamental freedoms.[3]

The international response also included the now-infamous trials in Nuremberg, Germany of Nazi doctors, scientists and others who had conducted non-consensual medical experiments on prisoners of war.[4] The Nuremberg medical trial for crimes against humanity concluded in the summer of 1947. In its judgement, the court outlined what became known as the *Nuremberg Code*, identifying "basic principles that must be observed in order to satisfy moral, ethical and legal concepts" in human experimentation.[5] While the Code outlines principles regarding the purposes of the research, the risks and benefits to the subject, and the duties and qualifications of researchers, its paramount principle states that "the voluntary consent of the human subject is absolutely essential." Because the major focus of the tribunal was on voluntary participation in human research, the Code does not include concepts such as privacy and confidentiality. Still, the Code stands as one of a collection of crucial post-WWII international human rights documents whose common spirit, international processes and shared dignitarian goals helped to define basic international standards for human research.

Indeed, within six months of the judgements in the medical trial at Nuremberg, the World Medical Association, the United Nations and European governments separately adopted a range of related formal declarations and legal instruments. These aimed to promote and preserve human dignity, in part by pledging commitment to the respect of individual freedom and autonomy, privacy and confidentiality. Each of these major legal and moral pronouncements thus contributed in its own way —directly or indirectly—to the collective result of enshrining privacy and autonomy principles as fundamental elements of the respect of human dignity in modern research. Pertinent highlights of the documents follow.

---

3 United Nations. *United Nations Charter,* Preamble. San Francisco: United Nations, June 1945.

4 *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10.*, Volume 2. Washington, DC: U.S. Government Printing Office, 1949, p. 181-182.

5 Annas G.J., Grodin M.A. *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation.* New York: Oxford University Press, 1992.

B. *Universal Declaration of Human Rights* (1948)

Within months of the conclusion of the Nuremberg Trials, the United Nations General Assembly adopted and proclaimed the *Universal Declaration of Human Rights (Universal Declaration)*.[6] The *Universal Declaration* is a recognition of and pledge to basic human rights for the international community. Its preamble deems "it essential that human rights be protected by law," and expresses some of the motivation behind this view:

> Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind …. Whereas the peoples of the United Nations have in the Charter (of the United Nations) reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person ….

The 30 articles of the *Universal Declaration* are diverse and non-binding. However, some of them have been given formal legal effect by their inclusion in both international human rights law and data protection treaties.

At least three articles of the *Universal Declaration* outline elements that would eventually be basic to data protection principles and laws that emerged decades later. Article 27 proclaims that "everyone has the right freely to participate in … scientific advancement and its benefits." The article expresses one of the core societal motivations and interests behind modern health science research.

Article 12 of the *Universal Declaration* identifies privacy as a basic human right, stating 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." Privacy legislation that has been adopted over the last decades is directly consistent with Article 12. Yet, what would happen if other principles and values expressed in the *Universal Declaration*—and thus other societal interests—were to conflict with or infringe on the right to privacy? The language of Article 12 provides some guidance. It proscribes only "arbitrary interference" with the right to privacy. As such, all infringements are not necessarily prohibited.

Article 29 of the *Universal Declaration* provides further guidance for dealing with such potential conflicts. It outlines how basic human rights may sometimes be limited:

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

The condition that any limitations be determined by law as justly required by other fundamental democratic principles expresses some of the standards and processes through which the international

[6] United Nations General Assembly. *Universal Declaration of Human Rights*. New York: United Nations, Adopted by Resolution 217A(III) of 10 December 1948. Online: http://www.unhchr.ch/udhr/lang/eng.htm

community might attempt to reconcile the commitment to privacy with other pressing societal needs. These elements would be drawn on and refined in subsequent laws, such as the *European Convention on Human Rights*.

C. *European Convention on Human Rights* (1950)

Two years after the UN proclaimed the *Universal Declaration*, the Council of Europe (COE) drew on some of its standards to define privacy as a fundamental principle of international law in the *Convention for the Protection of Human Rights and Fundamental Freedoms: European Convention on Human Rights* (ECHR).[7] Founded by treaty in 1949 as an intra-European human rights organization, the COE originally consisted of some 10 nations. Today, the ECHR is in effect in approximately 40 COE member nations that have adopted it.[8] Those nations are required to ensure that domestic law comports with the principles of the ECHR.

Drawing on the *Universal Declaration,* Article 8 of the ECHR outlines the right of privacy and limits thereon:

> Everyone has the right to respect for his private and family life …. 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.

While Article 8 of the ECHR adopts the substance and much of the language of articles 12 and 29 of the *Universal Declaration*, it makes some noteworthy refinements. It adds an explicit requirement that infringements must be justified in accordance with law and be shown "necessary" in a democratic society. The ECHR also adds the explicit grounds of the "protection of health or morals" to the list of democratic necessities that may sometimes require infringements on privacy. As will be shown in Section III, below, the necessity test and protection of health grounds would be adopted decades later into international data protection laws and principles.

The ECHR has helped to make the protection of privacy enforceable as a matter of international human rights law. Under the treaty, for instance, individuals in COE member nations who judge that national laws or practices violate the Article 8 right to privacy may have recourse to the COE. After exhausting legal remedies in one's country, one may file a human rights complaint by petitioning the COE European Court of Human Rights. Through cases that have thus alleged the wrongful disclosure of personal health data, for instance, the court has begun to interpret this dimension of

---

7 Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms.* Rome, 4 November 1950. E.T.S. No. 5, 213 U.N.T.S. 222. Online: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

8 Member states include Albania, Andorra, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, the "former Yugoslav Republic of Macedonia," Turkey, Ukraine, and the United Kingdom.

the right to privacy. It has observed "that the protection of personal data … [i]s of fundamental importance to a person's enjoyment of his or her right to respect for private and family life … ; accordingly, 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."[9] Such cases underline the role of the courts in the societal effort to define standards for the collection, use and disclosure of personal health data in a manner that is consistent with respect for human privacy.

D. International Covenants (1966, 1976)

International Covenants on Civil and Political Rights and *International Covenant on Economic, Social and Cultural Rights* (1966, 1976)

The respect of privacy as a fundamental principle of international law was formally integrated into the broader international community in 1966, when the UN General Assembly adopted and opened for signature the *International Covenant on Civil and Political Rights* (CCPR).[10] That same year, the UN also adopted a companion document, the *International Covenant on Economic, Social and Cultural Rights* (CESC).[11] These covenants, as binding international treaties, were intended to elaborate on, and give formal legal effect and implementation to, the principles proclaimed in the *Universal Declaration*. The covenants took effect in 1976. They have been signed and ratified by over 140 nations.

At least three articles from the covenants would prove directly relevant to subsequent international data protection laws and principles. These articles address privacy, consent, research and health.

First, Article 17 of the CCPR outlines the right to privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy …. Everyone has the right to the protection of the law against such interference or attacks." The provision thus adopts verbatim the language of Article 12 of the *Universal Declaration*. Yet, in contrast to both Article 29 of the *Universal Declaration* and Article 8 of the ECHR, the CCPR is silent on the standards for limiting the right to privacy.

Secondly, and again in contrast to both the *Universal Declaration* and ECHR, the CCPR gives explicit legal effect to the *Nuremberg Code*. Article 7 provides that "no one shall be subjected without his free consent to medical or scientific experimentation."

Thirdly, articles 15 and 12 of the CESC respectively include, in the enumeration of social rights, the right of everyone to enjoy "the benefits of scientific progress and its applications" and "the highest attainable standard of physical and mental health." Both are drawn from the *Universal Declaration*. Article 15 further provides that nations signing the CESC "undertake to respect the freedom indispensable for scientific research."

---

[10] United Nations, General Assembly. Resolution 2200A of 16 December 1966: *International Covenant on Civil and Political Rights*, adopted and opened for signature, ratification and accession. Can. T.S. 1976 No.47, 999 U.N.T.S. 171. Online: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

[11] United Nations, General Assembly. Resolution 2200A (XXI) of 16 December 1966: *International Covenant on Economic, Social and Cultural Rights*, adopted and opened for signature, ratification and accession.

Whether or not these latter provisions regarding scientific research and health in the CESC are to be accorded equal status to the rights of privacy and consent in the CCPR, the inclusion of all four principles in international treaties in the 1970s formally expresses their relevance and value in the promotion and protection of human dignity. It would be left to privacy laws and data protection principles from the 1970s onward to define more precise standards, definitions, structures and processes to balance the protection of privacy and the legitimate use of personal data for health research.

E. *Declaration of Geneva* (1948) and *Declarations of Helsinki* (1964, 1975 and 2000)

The World Medical Association (WMA), founded in 1947, is an international association that promotes high international standards of conduct for physicians. It has done so over the years through a range of formal declarations, statements and resolutions. Three are of particular relevance to international privacy and research norms.

First, in 1948, some six months after the close of the Nuremberg trials, the WMA adopted the *Declaration of Geneva*.[12] The *Declaration of Geneva* is a physician's oath that was later adopted into a WMA *International Code of Ethics*. The *Declaration of Geneva* begins with a solemn pledge to devote life to the service of humanity. It then lists several responsibilities, including a duty to "respect the secrets which are confided in me, even after the patient has died." This post-mortem duty of confidentiality would be incorporated into the data protection guidelines of the United Nations in 1990.

The second relevant WMA declaration came over a quarter of a century after the 1948 *Declaration of Geneva*. In 1964, the WMA adopted a detailed declaration on ethical principles for medical research that became known as the *Declaration of Helsinki*.[13] Responding in part to the heritage of Nuremberg, the *Declaration of Helsinki* largely concerned research procedures, risk assessment duties, and issues of informed consent to participating in human research. The 1964 declaration was silent on issues of privacy or confidentiality. However, when the *Declaration of Helsinki* was amended in 1975, it expressly included privacy: "The right of the subject to safeguard his integrity must always be respected. Every precaution should be taken to respect the privacy of the subject …." The year-2000 revision of the declaration, which retains this language, has added a more general duty: "It is the duty of the physician in medical research to protect the life, health and privacy and dignity of human subjects."[14] As manifested by the *Declaration of Helsinki* since at least the mid-1970s, privacy and informed consent are considered central to preserving the integrity and dignity of human subjects. Both have been explicitly recognized as international medical ethics norms for the conduct of research. The inclusion of privacy and consent into formal international documents dealing with the ethics of human research parallels the formal recognition of these norms in the CCPR, from the same era.

---

12 World Medical Association. *Declaration of Geneva: A Physician's Oath*. Geneva, 1948, as amended.

13 World Medical Association. *Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects.* Helsinki, 1964; art. III.4a.

14 World Medical Association. *Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects.* Edinburgh, 2000; arts. B.10, B.21. Online: www.wma.net

In retrospect, a third WMA declaration may help to explain the 1975 amendment to the *Declaration of Helsinki* that expressly included respect for privacy in the context of medical research. That amendment followed statements related to privacy that the WMA adopted in 1973. In considering the benefits and burdens of the advent of computers in medicine at its World Medical Assembly in 1973, the WMA adopted resolutions that, among other things, reaffirmed "the vital importance of maintaining medical secrecy … for the protection of the privacy of the individual as the basis for the confidential relation between the patient and his doctor."[15] The resolution directly linked professional duties of confidentiality with privacy. Today, in its amended version, the WMA *Statement on the Use of Computers in Medicine*[16] seeks to harmonize the duty to respect confidentiality, as proclaimed in the WMA *Declaration of Geneva*, with health research that may be facilitated by electronic data processing. The statement provides that it "is not a breach of confidentiality to release or transfer confidential health care information required for the purpose of conducting scientific research … provided the information released does not identify, directly or indirectly, any individual patient in any report of such research … or otherwise disclose patient identities in any manner …." The details and definitions in the WMA *Statement on the Use of Computers in Medicine* are characteristic of the early data protection principles and laws of the 1970s and 1980s.

[15] World Medical Association. The 27th World Medical Assembly: Munich October 14-20, 1973. *World Med. J*,1974; 21(1):4-10.

[16] World Medical Association. *Statement on the Use of Computers in Medicine*, based on Resolution of the 27th World Medical Assembly in Munich, Germany, October 1973, as amended by the 35th World Medical Assembly in Venice, Italy, October 1983.

III. Modern International Data Protection Principles and Laws (1980s to the Present)

This section outlines modern international data protection principles and laws that were developed beginning in the 1980s. These principles and laws, based on the foundational international privacy standards articulated between 1945 and the 1970s, craft specific and detailed standards for balancing legitimate societal uses of personal information with the respect for the right to privacy. Many of these data protection standards draw on general leading principles that were outlined early in the 1980s. Countries have since tended to refine and apply them to particular areas, such as research involving personal health information. The standards sampled below include those from the Organization for Economic Co-operation and Development, the Council of Europe, the European Union and the United Nations.

A. Organization for Economic Co-operation and Development (OECD)

1. *OECD, Personal Data Protection Principles (1980)*

Founded by international treaty in 1960, the Organization for Economic Co-operation and Development (OECD) outlined an influential set of data protection principles in 1980. The principles, contained in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[17] (*OECD Guidelines*), include the following:

- Collection Limitation Principle
- Data Quality Principle
- Specification of Purpose Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

The principles have been influential in subsequent international and national documents on data protection, and in the deliberations, public policy, and laws of some 30 member nations[18] of the OECD. The preface to the *OECD Guidelines* indicates that about half of the OECD countries had enacted, or were about to enact, data privacy legislation when the *OECD Guidelines* were adopted. The *OECD Guidelines* are not legally binding. They attempt to clarify international consensus on data protection principles as reflected in the legislation of member states. In attempting to develop guidelines to harmonize evolving national privacy and data protection laws, the preface of the *OECD Guidelines* addresses the challenge of preventing

[17] OECD, *Guidelines on the Protection on Privacy and Transborder Flows of Personal Data* OECD: Paris, 1981. Online: www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

[18] Member states include Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Online: www.oecd.org

violations of fundamental human rights that could result from the unlawful storage or unauthorized use and disclosure of personal data, while not hampering the free flow of legitimate personal data across international borders and through national economies that increasingly depend on information and communications technology. Highlights of the *OECD Guidelines* follow.

a. Scope

The standards in the *OECD Guidelines* apply to personal data in both the public and private sectors. Article 2 indicates that the standards apply only to data that by their nature, context of use, or manner of processing "pose a danger to privacy or individual liberties."

b. Definitions

Article 1 of the *OECD Guidelines* defines "personal data'' as ''any information relating to an identified or identifiable individual." No further definition of "identifiable individual" is elaborated. However, paragraph 43 of the Explanatory Memorandum for the guidelines notes that non-identifying data, such as statistical or anonymous data, are not implicated.

c. Special Protections: Sensitive Data

In contrast to then-existing and subsequent international data protection standards, the *OECD Guidelines* do not outline special protections for particular categories of data, such as personal health information. Article 3 of the *OECD Guidelines* makes it clear that they are not to be interpreted as preventing the development of "different protective measures." The Explanatory Memorandum that accompanies the guidelines notes that the drafters pondered the sensitive data issue. However, the memorandum expressed doubt on whether particular kinds of data are universally regarded as being sensitive and whether individuals associated with particular groups (for example, persons with mental disability) and sensitive data actually need additional protection. (See paragraphs 19 and 32.) In the subsequent two decades, though, the standards adopted by other international organizations tend to have resolved such doubts in favour of heightened protection for sensitive data.

d. Consent: Data Collection, Use and Disclosure

The Guidelines require consent as a foundational element for the collection of personal data. In outlining the data collection limitation principle, Article 7 indicates that personal data should be collected by fair and lawful means, "and where appropriate, with the knowledge or consent" of the person about whom the data are being collected. This data collection limitation principle functions in concert with other related principles. Articles 8 to 10 of the *OECD Guidelines* also outline "purpose specification," "data quality" and "use limitation" principles. Together, the standards mean that only relevant and accurate data should be collected for precise and limited purposes, and that disclosure and use should be restricted to those original purposes unless consented to by the data subject or authorized by law. The requirement for consent or legal authorization thus protects privacy and advances legitimate collection, use and disclosure of personal information.

e. Exceptions and Research

Article 4 of the *OECD Guidelines* offers guidance on making exceptions to the general duties of data protection. It indicates that exceptions to the general duties on grounds such as national

security or public order should be " as few as possible" and be "made known to the public." These provisions seem to reflect two intentions: first, to give broad effect to the protection of privacy while avoiding undue and countless exceptions that might jeopardize the very purposes and values of such protection; second, to make such exceptions transparent and publicly known so that they may be subject to the normal scrutiny, debate and accountability of a democratic society.

Though not directly mentioned in the principles themselves, paragraph 47 of the Explanatory Memorandum for the *OECD Guidelines* does indicate that these guidelines were written on the assumption "that exceptions will be limited to those which are necessary in a democratic society." The *OECD Guidelines* do not specifically address health or scientific research and outline no specific exceptions for health research.

f. Data Retention and Security

Article 11 of the *OECD Guidelines* explains the Security Principle by calling for personal data to be protected by "reasonable security safeguards" against accidental destruction or loss and unauthorized access, alteration or disclosure. Reasonable security safeguards may include, as paragraph 56 of the Explanatory Memorandum notes, physical measures that control access, organizational measures such as codes of conduct for institutional data collectors, and information technology measures such as enciphering. The *OECD Guidelines* do not specify a precise length of time for data retention. Rather, the principles for limiting data collection to specified purposes and limited uses seem to imply that the length of data retention depends on whether the data continue to be necessary to fulfil the specified purpose(s).[19]

g. Other Noteworthy Provisions

The *OECD Guidelines* encourage nations to undertake initiatives, both national and international, to protect the privacy of personal data.

Within their own borders, nations are encouraged to "establish legal, administrative or other procedures or institutions." In particular, this means to endeavour to adopt appropriate legislation, support self-regulation, provide reasonable means for individuals to exercise their rights, provide adequate sanctions and remedies, and ensure that no unfair discrimination occurs.

For international implementation, member nations are urged to cooperate with one another to facilitate the free flow of personal data and define legitimate restrictions. This challenge does involve some balancing. On one hand, Article 18 urges member nations not to unduly restrict data flow by establishing excessive privacy standards. On the other hand, Article 17 provides that member countries may impose restrictions on transfers to other nations, given the nature of the data and given a lack of "equivalent protection" in other countries. As did many of the concepts and principles in the *OECD Guidelines*, the equivalent protection concept became a legal standard central to international data protection law and policy some two decades later.

[19] Organization for Economic Co-operation and Development (OECD). *Explanatory Memorandum, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, para. 54-55. Paris: OECD, 1981. Online: www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

B. Council of Europe (COE)

As is mentioned in Section II.C, the Council of Europe was founded in the late 1940s as an intra-European human rights organization.[20] Complementing the privacy protection provision of the ECHR, at least three documents outline modern health data protection standards of the COE. These include the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981) (*COE Convention 108/1981*), the *Recommendation on the Protection of Medical Data* (1997) *(COE Recommendation R97[5])*, and the *Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine* (1997) *(Convention on Human Rights and Biomedicine)*.

1. *COE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)*

In 1981, following initial work in the early 1970s on the protection of privacy regarding electronic data banks, the COE opened for signature the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (*COE Convention 108/1981*).[21] Like the *OECD Guidelines*, the document addresses a basic societal challenge. Its preamble announces the task of reconciling "the fundamental values of respect for privacy and the free flow of information between peoples." In contrast to the *OECD Guidelines*, the convention is binding as an international treaty. It obliges the 20 European nations that have adopted it to harmonize their laws to give effect to the principles outlined in it. Non-member countries of the COE may also accede to the *COE Convention 108/1981*. Selected highlights follow.

a. Scope

Article 3 of the *COE Convention 108/1981* indicates that it applies to automated personal data files and automatic processing of personal data. The article gives member states the discretion to extend the principles to non-automatic processing. However, by virtue of its limited application to the automatic processing of data, it is thus narrower in scope than the *OECD Guidelines*. Like the *OECD Guidelines*, it applies to both the public and private sectors.

b. Definitions

Article 1 of the *COE Convention 108/1981*, like the *OECD Guidelines*, defines "personal data" as "any information relating to an identified or identifiable individual." It offers no definition of identifiable individual. It defines "automatic processing" as including the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, and their alteration, erasure, retrieval or dissemination.

---

[20] Member states include Albania, Andorra, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, the Russian Federation, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, the "former Yugoslav Republic of Macedonia," Turkey, Ukraine and the United Kingdom.

[21] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, *E.T.S. No. 108*. Strasbourg, 28 January 1991. Online: http://conventions.coe.int/treaty/en/Treaties/html/108.htm

c. Special Protections: Sensitive Data

Article 6 of the *COE Convention 108/1981* outlines additional protections for "special categories of data." It thus diverges from the *OECD Guidelines*. The *COE Convention 108/1981* provides that personal data concerning racial origin, religious beliefs, health or sexual life "may not be automatically processed unless domestic laws provide appropriate safeguards." The document itself does not elaborate on or illustrate such appropriate safeguards. Nor does it explicitly require the consent of the data subject for processing sensitive data. Still, the *COE Convention 108/1981* does require special protection for personal data of a sensitive nature. In doing so, the *COE Convention 108/1981* set a standard that would be subsequently adopted by other organizations in international data protection law.

d. Consent: Data Collection, Use and Disclosure

For general or non-sensitive personal data, Article 5 indicates that personal data must generally be processed fairly and lawfully, be stored for a specified and legitimate purpose, and be accurate, relevant, and not excessive in relation to the purpose for its storage. In contrast to the *OECD Guidelines*, these general provisions contain no express requirement for the informed consent of the person about whom the information is being processed. An explicit consent requirement might nonetheless arise under national law.

e. Exceptions and Research

Article 9 of the *COE Convention 108/1981* provides exceptions to the general duties regarding data protection. While the *OECD Guidelines* indicate that the exceptions should be "as few as possible," the COE indicates that such exceptions should be "necessary" for such democratic societal needs as state security, public safety, or the suppression of criminal activity. The *COE Convention 108/1981* does not provide for the processing of data for research purposes. However, interestingly, Article 9.3 indicates that national laws may limit the data subject's right of access to and correction of automated personal data used for scientific research and statistical analysis when "there is obviously no risk of an infringement of the privacy of the data subjects."

f. Data Retention and Security

Article 7 of the *COE Convention 108/1981* calls for "appropriate security measures" to be undertaken to protect data against accidental destruction or loss and unauthorized access, alteration or disclosure. This parallels the *OECD Guidelines*. Article 5.e indicates that identifiable data are to be preserved no longer than is required for the purpose for which the data are stored. This provision parallels the implied rationale of the *OECD Guidelines* on the length of data retention.

g. Other Noteworthy Provisions

The *COE Convention 108/1981* contains important provisions for its implementation nationally and internationally. Article 12 parallels the *OECD Guidelines* by authorizing restrictions on international data transfers to countries lacking "equivalent protection" in privacy norms. For domestic implementation, Article 10 requires nations to provide "appropriate sanctions and remedies" for violations of national laws that express the principles of the *COE Convention 108/1981*. However, in contrast to more recent data protection principles of the United Nations and European Union (see sections III. C and D, below), the original *COE Convention 108/1981* includes no specific requirement for the establishment of national data protection supervisory

authorities. Accordingly, an amendment to the *COE Convention 108/1981* has recently been proposed.[22] It would require countries to establish independent supervisory authorities responsible for ensuring compliance with conforming legislation or regulations introduced by the states. Finally, articles 18 and 19 of the *COE Convention 108/1981* create an advisory committee that, among other things, is responsible for recommending reforms and responding to written queries on the *COE Convention 108/1981*. The proposed amendment on national supervisory authorities emerged in part from the deliberations of this advisory committee.

2. *COE Recommendation on the Protection of Medical Data (1997)*

To contour and elaborate the general principles of the *COE Convention 108/1981* (1981) to the specific needs of various sectors of society, the COE has over the years proposed a number of recommendations. These have addressed issues such as medical databanks (1981), scientific and other statistical research (1983), data transfers by public institutions (1991), and data processed for statistical purposes (1997). Such recommendations are not legally binding. Rather, they reflect a COE request to member states to consider, in good faith, the implementation of national law in conformity with recommended applications and interpretations of the *COE Convention 108/1981*. As such, the recommendations detail standards of reference on precise data protection issues for the COE community. In 1997, the COE adopted *Recommendation R97(5) on the Protection of Medical Data (COE Recommendation R97[5])*,[23] which addresses medical research in some detail. Many of its provisions are inspired by the *OECD Guidelines*, the *COE Convention 108/1981,* and the EU *Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (EU Privacy Directive).*

a. Scope

Article 2 indicates that *COE Recommendation R97(5)* applies to the collection and automatic processing of medical data in particular. Its limitation to the automatic processing of medical data is thus even narrower than both the *OECD Guidelines* and the *COE Convention 108/1981*. The Article gives member states the discretion to extend its principles to non-automatic processing. Like the *OECD Guidelines* and *COE Convention 108/1981*, it applies to both the public and private sectors.

b. Definitions

Among other things, *COE Recommendation R97(5)* contains definitions of "personal data", "identifiable individual", and "medical data". Like the *COE Convention 108/1981* and *OECD Guidelines*, Article 1 defines "personal data'' as "any information relating to an identified or identifiable individual." It differs from the *COE Convention 108/1981* and *OECD Guidelines* in that it also defines "identifiable" as follows: "an individual shall not be regarded as 'identifiable'

[22] Council of Europe. *Draft Additional Protocol to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (E.T.S. No 108) Regarding Supervisory Authorities and Transborder Data Flows and Explanatory Report.* Strasbourg, 2000. Online: http://stars.coe.fr/index_e.htm

[23] Council of Europe. *Recommendation No. R97(5) of the Committee of Ministers to Member States on the Protection of Medical Data*. Strasbourg, 1997. Online: http://cm.coe.int/ta/rec/1997/97r5.html

if identification requires an unreasonable amount of time and manpower." Article 1 also specifically defines medical data as "all personal data concerning the health of an individual." It refers to data that have a clear and close link with health, as well as to genetic data.

c. Special Protections: Sensitive Data

COE Recommendation R97(5) explicitly draws on Article 6 of the *COE Convention 108/1981*. Article 6 outlines special protections for personal data concerning health. As such, the *Recommendation R97 (5)* extends the rationale of the article into a detailed statement of special standards. It even outlines standards for some subsets of medical information, such as genetic data.

d. Consent: Data Collection, Use and Disclosure

Like the *COE Convention 108/1981* and the *OECD Guidelines*, Article 4 indicates that medical data must generally be processed fairly and lawfully, and only for a specified purpose. In contrast to the *COE Convention 108/1981*, however, *COE Recommendation R97(5)* includes consent as an explicit condition for the processing of medical data. This parallels the *OECD Guidelines* and the *EU Privacy Directive*. Article 4.3 of *COE Recommendation 97(5)* provides that medical data may generally be collected or processed if valid consent has been obtained or if the law otherwise provides for non-consensual data collection. Consent may be given by (a) the data subject, or (b) her or his legal representative, or (c) other lawful authority. A valid consent, according to Article 6, needs to be "free, express and informed." Article 5 identifies basic informational elements that should be shared with the data subject and thus contribute to informed consent. Article 8 outlines similar standards for communication and disclosure.

e. Exceptions and Research

COE Recommendation R97(5) also outlines standards for non-consensual processing of medical data, including research. As in other documents, the exceptions are generally structured and crafted narrowly on a necessity standard that expresses competing and sometimes overriding societal interests. Articles 4 and 7 specifically define norms for the non-consensual "collection" and "communication" of medical data. Though "communication" is not defined, its provisions target the disclosure or sharing of medical data. Both articles 4 and 7 indicate that medical data may be collected and communicated without consent, when "authorized by law" for public health reasons, for preventing real dangers, or for similarly important public interests. Data may also be collected or communicated when "permitted by law" for, among other things, contractual matters, legal proceedings, safeguarding vital interests of a person, or for the therapeutic purposes of the data subject or her or his genetically related relative. These provisions parallel the standards of the *EU Privacy Directive***.**

Beyond the latter provisions, *COE Recommendation R97(5)* also details particular duties and exceptions for the use of medical data in research. Article 12 specifies a general duty to be sure that medical data for research remain anonymous. Use of identifying medical data is authorized under certain conditions. It must be shown that the research project needs to be carried out for "legitimate purposes" and that anonymization of the medical data would make the research project "impossible." Once legitimate purposes and impossibility have been shown, use may proceed (a) with the consent of the data subject or a legal representative thereof, or (b) with authorization from a duly and lawfully authorized entity under particular criteria, or (c) when the research is necessary for public health reasons and authorized by law. In keeping with

COE Convention 108/1981, Article 8.2 of the *COE Recommendation R97(5)* limits a data subject's general right of access to medical data used for scientific research and statistical research purposes when "there is clearly no risk of an infringement" on privacy.

f. Data Retention and Security

Article 9 of *COE Recommendation R97(5)* generally echoes the basic security standards of the *COE Convention 108/1981* and the *OECD Guidelines*. In addition, Article 9 details a range of "appropriate measures" that should be periodically reviewed to ensure the confidentiality and accuracy of processed data. These include controls over memory, communication, transport, data entry and use, as well as processing designed to separate identifiers from administrative, social and medical data.

Consistent with the *COE Convention 108/1981* and the *OECD Guidelines*, Article 10 of *COE Recommendation R97(5)* outlines a general duty to retain data no longer than necessary to achieve the purpose for which it was collected. The general duty is subject to two exceptions: first, if it is otherwise "necessary" to preserve the data for, among other things, legitimate interests of public health, medical sciences, or historical or statistical research, "taking into account the privacy of the patient." Secondly, requests by individuals to have personally identifiable medical data destroyed should generally be honoured, unless an "overriding and legitimate interest" or superseding obligation justifies its conservation. Data made anonymous need not to be destroyed.

g. Other Noteworthy Provisions

Beyond its specific focus on the automatic processing of medical data, *COE Recommendation R(97)5* contains a few other noteworthy dimensions. First, it is intended to supersede the *COE Recommendation 1981* on automated medical banks and reflect more current thinking in light of recent developments, including parallel initiatives by the EU as reflected in the *EU Privacy Directive*. (See Section C.1, below.) Second, *COE Recommendation R97(5)* indicates that, as a general rule, international transfers of medical data between COE nations should be evaluated on whether a recipient nation has "equivalent protection" to the provisions and principles of *COE Recommendation R97(5)*. It remains to be seen whether the "equivalent protection" standard of *COE Recommendation R97(5)* will be substantively similar to, or different from, the "adequate protection" standard of the *OECD Guidelines* and the *EU Privacy Directive.* (See Section C.1, below.)

3. *COE Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine (1997)*

In the 1990s, the COE became one of the first international organizations to attempt to define a formal treaty that addresses the protection of human rights in the face of "accelerating developments in biology and medicine." The initiative draws on the heritage of the *Universal Declaration* and the ECHR to erect legal approaches aimed at furthering human dignity in modern society. In 1997, the *COE Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine (1997) (COE*

Convention on Human Rights and Biomedicine)[24] was opened for signature. Over half of the Council's 41 member countries have signed the Convention. It is also open to non-member nations, such as Australia, Canada, Japan and the United States, that had observer status in the COE Steering Committee on Bioethics.

At least four of its provisions generally involve health research and privacy. First, Article 15 announces the principle that scientific research in the field of biology and medicine shall be carried out freely, subject to provisions in the Convention and other legal instruments for "ensuring the protection of the human being." Second, Article 16 then outlines general standards governing research on a person. They include independent review of the scientific merit and ethical acceptability of the project, informed consent of the participant, and, as a part of the informed consent process, advising potential participants of their rights and legal protections. Such rights and protections are elaborated by the Convention's specific provisions on informed consent and privacy. Third, then, the Convention includes an express provision on the protection of privacy. Article 10 provides that "everyone has the right to respect for private life in relation to information about his or her health." Fourth, the article indicates that the right to privacy includes an entitlement of choice: to know, or to decline to be informed, of information collected about one's health. The *COE Convention on Human Rights and Biomedicine* does not contain an explicit data protection provision, though it does refer to the *COE Convention 108/1981*. More specificity may emerge from formal amendments to the *COE Convention on Human Rights and Biomedicine* in the form of protocols. Protocols, which tend to focus on more specific issues, have been drafted for cloning and organ transplantation. Further protocols are currently being prepared for medical research and for genetics.

C. European Union (EU)

Created by international treaty in the 1950s, the European Economic Community (EEC) has promoted and harmonized laws and policy on economic relations, trade and development in Europe over the years. Some of its harmonization policies have indirectly touched on scientific development, research and health. Examples include the longstanding EEC initiatives on the harmonization of pharmaceutical and patent law. Under a new treaty adopted in the 1990s, the EEC changed its name to the European Union and broadened its mandate. It now explicitly includes health matters in its mandate. Members of the EU include some 15 European nations.[25] Because member states are required to harmonize their laws with EU directives and like legal requirements, the EU has powers, roles and responsibilities akin to a federal government for much of Europe. Its inter-European roles are discharged largely through the European Parliament, the European Court of Justice, the European Council, and the European Commission.

---

[24] 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*, E.T.S. No.164. Oviedo, 1997. Online: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm

[25] Member states, as of spring 2001, include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. Membership is expected to expand.

In this context, between 1995 and 2000, the EU adopted three formal documents that outline modern data protection principles for personal health information. They are: 1) the *European Union Privacy Directive* (1995), 2) an *Opinion on Health Care in the Information Society* (1999) and 3) the *European Union Charter of Fundamental Rights* (2000).

1. *European Union Privacy Directive (1995)*

EU *Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* (*EU Privacy Directive*) entered into force in 1998.[26] Member states are obliged to bring their national laws into conformity with the principles of the *EU Privacy Directive* within three years of its adoption. In order to do so, they may employ whatever instruments of law (statutes, regulations, decrees, etc.) they deem appropriate. The Directive has yielded new or revised data protection laws in many European nations, including Greece, Italy, Portugal, Switzerland, the United Kingdom, Germany, Austria, Belgium, Spain, Denmark, Finland and the Netherlands. The Directive shares the twin goals of the *OECD Guidelines* and the *COE Convention 108/1981*: to protect the fundamental right to privacy in the processing of personal data and to harmonize the free flow of such data between nations.

a. Scope

According to its Article 3, the *EU Privacy Directive* applies to the processing of personal data by automated or non-automated means. It thus parallels the scope of the *OECD Guidelines* and is broader than the *COE Convention 108/1981*. Like the *OECD Guidelines* and the *COE Convention 108/1981*, the *EU Privacy Directive* applies to data in both the public and private sectors.

b. Definitions

Article 2 of the *EU Privacy Directive*, like the *OECD Guidelines*, defines "personal data'' as "any information relating to an identified or identifiable individual." However, in contrast to the *OECD Guidelines* and the *COE Convention 108/1981*, the *EU Privacy Directive* further defines an "identifiable individual" as a person 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. According to Article 2 of the Directive, "processing" of personal data includes the collection, storage, consultation, use, disclosure, alteration or destruction of personal data.

c. Special Protections: Sensitive Data

Like the *COE Convention 108/1981* and unlike the *OECD Guidelines*, the *EU Privacy Directive* explicitly offers higher standards for the processing of "special categories of data," including identifiable health information. It does so, in part, by imposing a general prohibition against the collection of health data, subject to some narrow exceptions. Article 8 specifically provides that EU member states "shall prohibit the collection of personal data concerning … health or

[26] *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 L 281, 23/11/1995 p. 0031 - 0050. Online: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

sexual life" unless the data subject has explicitly given a free, specific and informed consent. Narrow exceptions to the general requirement of consent are outlined below, in Section 1.e.

d. Consent: Data Collection, Use and Disclosure Standards

For the processing of general personal data, the Directive outlines both data quality principles and consent standards. Article 6 indicates, among other things, that personal data must generally be (a) processed fairly and lawfully, (b) collected for a specified, explicit and legitimate purpose and (c) accurate and relevant. These echo the original OECD quality control principles, with minor and sometimes important innovations.

For instance, the Directive builds on the specified and legitimate purpose principle of the *OECD Guidelines* by adding the requirement that the purpose be "explicit." The requirement of an explicit purpose theoretically enables those about whom the data are being collected to provide more detailed, precise and informed consent to their collection and use. This requirement is complemented by articles 11 to 13, which require additional information to be given to the data subject about his or her right of access, right to rectify data, and rights to have information about particular data collected. The *EU Privacy Directive* also adds important elements to the consent standard for the collection of personal data. While the *OECD Guidelines* indicate that data collection may proceed with the knowledge and consent of the data subject "where appropriate," the *EU Privacy Directive* outlines a basic consent requirement in more certain terms. More specifically, Article 7 provides that personal data may be processed "only if the data subject has unambiguously given consent" subject to an explicit necessary standard. (See Section E, below.) "Consent," as defined in Article 2 of the *EU Privacy Directive*, is a voluntary, specific and informed indication of agreement to the processing of personal data.

e. Exceptions and Research

The *EU Privacy Directive* outlines three categories of exceptions based on a necessity standard—that is, a requirement that the exceptions be demonstrably necessary to advance a competing or overriding societal interest. The test mirrors the necessity standards of the *COE Convention 108/1981* and the *OECD Guidelines*.

First, Article 7 indicates that in the absence of consent, non-consensual processing of general personal data must be shown to be necessary for, among other things, complying with a legal obligation under national law, protecting interests of the data subject, or undertaking a task in the public interest.

Second, Article 8 provides more specific consent rules and exceptions for the processing of sensitive data such as personal health information.

Article 8 indicates that, beyond the general conditions that must be met for the processing of general personal data, particular conditions for the exceptional processing of health data without consent require demonstration that the processing is necessary to advance a "substantial public interest," such as the defence of legal claims or for therapeutic purposes such as diagnosis, care, treatment or health care services management. The societal benefits of scientific research may persuade some European states to define health research as a substantial public interest exception necessary for the advancement and promotion of biomedical, epidemiological, geno-

mic, public health and like research. Even so, non-consensual data processing of identifiable health data for research purposes would still have to comply with an additional privacy standard in Article 8 of the Directive; that is, that health data be processed only by those subject to a professional obligation of confidentiality or secrecy or the equivalent thereof.

Third, Article 13 outlines general exemptions that member states may adopt legislatively as legitimate restrictions on the data quality standards, on the information that must be disclosed to data subjects, and on rights of access and correction to data. The restriction must constitute a necessary measure to safeguard national defence, the administration of criminal justice, or an important financial interest of a member state. Although the *EU Privacy Directive* makes no specific reference to a research exception for non-consensual processing of general personal data or health data, Article 13 indicates that national laws with adequate safeguards may limit the data subject's right of access to and correction of personal data processed solely for scientific research when "there is clearly no risk of breaching the privacy of the data subjects." This parallels the similar exception in the *COE Convention 108/1981*.

f. Data Retention and Security

Article 17 of the *EU Privacy Directive* generally calls for "appropriate technical and organizational measures" to be undertaken to protect data against accidental destruction or loss, and unauthorized access, alteration or disclosure. This parallels OECD standards. The article prescribes a balancing standard: even acknowledging cost and technological factors, the level of security should be proportionate to the risks associated with the nature and processing of the data. Like the *COE Convention 108/1981*, Article 6.e of the *EU Privacy Directive* indicates that identifiable data are to be preserved no longer than is required for the purpose for which the data were collected. Article 6.e also calls on countries to outline appropriate safeguards for personal data stored for longer periods for statistical or scientific research purposes.

g. Other Noteworthy Provisions

The *EU Privacy Directive* outlines a number of provisions that affect implementation nationally, within the EU, and internationally. For example, member states are obliged to ensure that national legislation includes enforcement and oversight mechanisms. Article 22 requires EU member states to ensure that individuals have legal recourse for violations of data protection rights. Article 28 further obliges member states to provide for independent national supervising authorities to oversee the monitoring and implementation of national data protection laws. To facilitate the implementation of the standards of the *EU Privacy Directive*, Article 27 obliges member states to encourage the development of data protection codes of conduct. For overall oversight and advice on the *EU Privacy Directive* and the evolution of data protection in the EU, Article 29 establishes an Independent Working Party.

The *EU Privacy Directive* also affects international data exchanges with non-EU nations. Article 25 obliges member states to provide that transfers to non-EU countries can take place only if recipient nations ensure an "adequate level of protection." An evaluation of the level of protection shall be judged on such factors as the nature of the data, relevant national laws, professional rules, and security measures. The determination is to be made by the Independent Working Party established by Article 29 of the *EU Privacy Directive*. Documents and reports on the evaluation of privacy protection standards in countries such as the US and Canada for

purposes of data sharing with EU member-states have recently been made public.[27] Article 26 of the *EU Privacy Directive* allows data-transfers to recipients in countries not certified as having adequate protection under limited circumstances. These include circumstances where the transfer is "necessary or required on important public interest" grounds. Finally, Article 33 indicates that the first three-year public report on the implementation of the *EU Privacy Directive*, potentially including proposed amendments, is due in autumn 2001.

2. *European Group on Ethics in Science and New Technologies: Ethical Issues of Healthcare in the Information Society, Opinion No. 13*

Founded originally under a different name in 1991, the European Group on Ethics in Science and New Technologies has a mandate to offer to the European Commission interdisciplinary ethics advice on issues occasioned by developments in science and technology. The European Group on Ethics in Science and New Technologies has released some 15 written opinions, many on ethical issues in biotechnology. In their 1999 advisory opinion on *Ethical Issues of Healthcare in the Information Society* (*European Group on Ethics Opinion*),[28] the Group addresses leading issues involved in the collection and use of personal health data for research.

In the *European Group on Ethics Opinion*, the Group adopts the eight original OECD data principles, and adds those of citizen participation and education. It identifies the tension between privacy and research as one of many value conflicts in the provision of health care. This tension had been noted in the *OECD Guidelines* and the *COE Convention 108/1981* some two decades earlier. Privacy, the *European Group on Ethics Opinion* suggests, may be traded for certain goods, such as research, under particular standards and conditions. Highlights of the *European Group on Ethics Opinion* follow.

a. Scope

The advisory *European Group on Ethics Opinion* addresses ethical issues of health care in the information society. It falls within the recently broadened EU mandate that now expressly includes health and human rights. The *European Group on Ethics Opinion* focuses on the use of identifiable health information for general health care purposes, including research.

b. Definitions

The Opinion adopts the definition of personally identifiable health data as defined in the *EU Privacy Directive*.

c. Special Protections: Sensitive Data

The *European Group on Ethics Opinion* notes that personal health data encompasses a wide range of information, including basic medical data (e.g., medical histories), sensitive data about mental health, or administrative data such as insurance information. The Opinion goes

---

[27] Online: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm. While reports and decisions on such countries as the US have been concluded, a final report and decision on Canada is expected early in 2002.

[28] European Group on Ethics in Science and New Technologies. *Ethical Issues of Healthcare in the Information Society, Opinion No. 13*. Brussels, 1999. Online: http://europa.eu.int/comm/secretariat_general/sgc/ethics/en/opinion13.pdf

on to state that "personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive …. Personal health data form part of the personality of the individual, and must not be treated as mere objects of commercial transaction."

Perhaps because it focuses only on health data, the *European Group on Ethics Opinion* does not specify how the protection of personal health data should compare with that of non-health personal data. Nor does it identify particular kinds of personal health information, such as genetics, as being more sensitive than others.

d. Consent: Data Collection, Use and Disclosure

The views and standards on consent are expressed in the Group's self-determination and confidentiality principles. Echoing the *OECD Guidelines*, Section 2.3 of the *European Group on Ethics Opinion* construes the principle of self-determination as including "citizens' right to know and to determine which personal health data are collected and recorded, to know who uses them for what purposes, and to correct data, if necessary." Furthermore, the citizen has a right to oppose any secondary use of his or her data that is not provided for by law.

Section 2.2 articulates a right to privacy and confidentiality, generally dependant on the individual's informed consent.

The human right to respect for private life requires that confidentiality of personal health data is guaranteed at all times. It also implies that, in principle, the informed consent of the individual is required for the collection and release of such data.

Consistent with the *EU Privacy Directive*, the section provides that all legitimate users of personal data have a duty of confidentiality *equivalent to* the professional duty of medical secrecy. Medical secrecy is seen as central to the trustworthiness of the health care system. Moreover, the *European Group on Ethics Opinion* adopts the position of the World Medical Association 1948 *Declaration of Geneva*: that the duty of confidentiality continues after the death of the person. (See Section II.E, above.)

e. Exceptions and Research

The *European Group on Ethics Opinion* does not provide expressly for a research exception, though it does provide that any exceptions to the duty of privacy and confidentiality "must be limited and provided for by legal rule." This approach parallels that of the *OECD Guidelines*. The use of personal data for the broad societal benefit must, moreover, be justified in the context of the individual's right to self-determination. Consistent with these principles, articles 2.2 and 2.3 infer that secondary uses of data should be narrow and specified in law.

f. Data Retention and Security

Article 2.6 deems the security of information and communication technologies "an ethical imperative." This imperative requires appropriate encryption technology, closed networks for personal data transfers, and organizational measures to support security. The *European Group on Ethics Opinion* does not specify a data retention period.

g. Other Noteworthy Provisions

The *European Group on Ethics Opinion* calls for the development of a specific directive on medical data protection within the framework of the *EU Privacy Directive*.

3. *European Union Charter of Fundamental Rights (2000)*

Under treaties adopted in the 1990s, member states of the EU have a binding legal obligation to respect fundamental human rights. The treaties make reference to the rights expressed in the ECHR, discussed in Section II. C, above. In 2000, the EU adopted a formal human rights document, the *European Union Charter of Fundamental Rights (EU Charter*).[29] It results from a common initiative in recent years to unite into one text the diverse civil, political, economic and social rights already reflected in diverse legal documents and sources within the broader EU community. As such, the *EU Charter* is broader than the ECHR. The *EU Charter* itself provides no directly enforceable legal remedy; it is not directly legally binding. Rather, similar to the *Universal Declaration*, it is a solemn proclamation of fundamental rights, evincing and reflecting general principles of EU law. In theory, then, the *EU Charter* may be referred to in judicial and legal proceedings as an interpretive source of EU human rights. Discussion and refinement of its formal status, and options such as its possible inclusion within the EU treaties, are to be deliberated over the next few years.

Article 7 of the *EU Charter* echoes the classic post-WWII call for incorporation of respect of privacy into human rights law by declaring that everyone has the "right to respect of his or her private and family life." It thus draws largely on the language of the *Universal Declaration*, the ECHR, and the CCPR and CESC. Though the article offers no definition of private life, the reference in the *EU Charter*'s preamble to some of these other international documents and to European human-rights case law indicates that "private life" is intended to be interpreted in a manner consistent with those standards.

The right to privacy is complemented by a brief and explicit data protection principle. Article 8 declares that "everyone has the right to the protection of personal data." Such data, the article continues, "shall be processed fairly for specified purposes and on the basis of consent or some other legitimate basis laid down in law." The inference is that exceptions to consensual data collection should be explicitly set forth in law. The article further calls for access by individuals as well as oversight of compliance by an independent authority. The *EU Charter* thus codifies leading elements of the original OECD data protection principles into a regional international human rights document.

D. United Nations (UN)

While Section II, above, indicates that the protection of privacy has, over the decades, been a central human rights concern in the international community, the United Nations (UN) began only in the 1990s to address in earnest the data protection dimensions of privacy. Since then, at least two

[29] European Parliament and Council. *Charter of Fundamental Rights.* Nice, 2000. Online: www.europarl.eu.int/charter/default_en.htm

initiatives of UN bodies have resulted in formal documents that address data protection: a 1990 resolution from the UN General Assembly and a 1994 declaration from a collaborative undertaking by a regional office of the World Health Organization.

1. *UN Guidelines on Computerized Personal Data Files (1990)*

In 1990, the UN General Assembly formally adopted *Guidelines for the Regulation of Computerized Personal Data Files (UN Guidelines).*[30] The *UN Guidelines* share and sometimes modify the original OECD norms by incorporating the following principles for the processing of computerized personal files: lawfulness and fairness, accuracy, purpose-specification, interested-person access, non-discrimination and security. The *UN Guidelines* are not binding. Still, they constitute a formal pronouncement by some 180 member states of the UN Generally Assembly. As such, they represent a high degree of consensus on, and evidence of, leading principles in international data protection law and policy.

a. Scope

The UN urges the *UN Guidelines* upon international governmental organizations, international non-governmental organizations, and nations as "minimum guarantees that should be provided in national legislation." The Guidelines apply to computerized personal files in the public and private domains. The *UN Guidelines* indicate that it is open to governments and organizations to apply them to manual files.

b. Definitions

The *UN Guidelines* do not define key terms used in the document.

c. Special Protection: Sensitive Data

In contrast to the *OECD Guidelines*, yet consistent with the *COE Convention 108/1981* and *EU Privacy Directive*, the *UN Guidelines* outline special protections for sensitive data. Subject to strict exceptions, the compilation of "data likely to give rise to unlawful or arbitrary discrimination" is generally prohibited. Data referring to an individual's sex life and racial or ethnic origin are referred to as examples of sensitive data, but the *UN Guidelines* do not explicitly include health data. Such designation is within the discretion of member nations.

d. Consent: Data Collection, Use and Disclosure

Under the *UN Guidelines*, data must be collected or processed lawfully and fairly, accurately, and for a specified and legitimate purpose. For purposes incompatible with those specified, use or disclosure of personal data generally requires the consent of the person concerned.

e. Exceptions and Research

The *UN Guidelines* provide for narrow exceptions to the general duties of lawful, fair and consensual collection, use and disclosure of personal data. Any exceptions must meet several conditions. They must be grounded on a necessity standard for the protection of, among other

[30] United Nations, General Assembly. *Resolution 45/95 of 14 December 1990*: *Guidelines for the Regulation of Computerized Personal Data Files.* New York, 1990. Online: http://www.unhchr.ch/html/menu3/b/71.htm

things, public order, public health or morality, national security, or the rights and freedoms of others. The exception must also be "specified in law" or in equivalent regulations and contained within express limits and "appropriate safeguards." The necessity standard parallels that of other international documents, such as the *OECD Guidelines*, the *COE Convention 108/1981*, and the *EU Privacy Directive*. For sensitive data, the *UN Guidelines* further require that any compelling exceptions respect the limits prescribed by relevant international human rights treaties and documents.

f. Data Retention and Security

The *UN Guidelines* parallel the *OECD Guidelines* for data security and retention. Personal data should be kept for a period not exceeding that necessary to achieve the specified and legitimate purpose for which it is kept. It should be protected by "appropriate" security measures from events such as accidental loss, destruction and unauthorized access.

g. Other Noteworthy Provisions

The *UN Guidelines* also directly address international data transfer and national implementation.

Like the *OECD Guidelines* and the *COE Convention 108/1981*, the *UN Guidelines* recommend that international data exchange should flow freely between countries that have "comparable safeguards" for the protection of privacy. Even where no such comparable safeguards exist, limitations on transborder data flows "may not be imposed unduly and only insofar as the protection of privacy demands."

For domestic implementation, the *UN Guidelines* go beyond the provisions of the *OECD Guidelines* and the *COE Convention 108/1981*, and outline standards that have since been adopted by the *EU Privacy Directive*. (See Section III.C.1, above.) The *UN Guidelines* recommend that national laws designate independent, impartial and technically competent national authorities to be responsible for supervising observance of the principles sanctioned by criminal or other penalties, together with appropriate individual remedies. In many counties, such responsibilities are now discharged by independent privacy commissioners.

2. *WHO Declaration on the Promotion of Patients' Rights in Europe (1994)*

In 1994, the World Health Organization (WHO) collaborated in convening a consultation to outline a common framework of principles for patients in Europe. The Consultation concluded by endorsing a formal regional *Declaration on the Promotion of Patients' Rights in Europe* (*WHO Declaration*).[31] Part of the intent of the *WHO Declaration* was that its principles of privacy, confidentiality and data protection would guide European governments in governing the health sector, and would be promoted and implemented through legislation, professional codes, training and education.

[31] World Health Organization European Consultation on the Rights of Patients. *A Declaration on the Promotion of Patients' Rights in Europe.* Amsterdam, March 1994.

The *WHO Declaration* advances privacy as a basic "human right and value" in health care. Article 1 declares that everyone has the right to self-determination, physical and mental integrity, and "respect for privacy." Consistent with the right to privacy in the health sector, Article 4.1 of the Declaration outlines the general duty to maintain confidentiality about patient health status, medical conditions, and "all other information of a personal kind"—even after death. The continuing post-mortem duty of confidentiality echoes that of the World Medical Association 1948 *Declaration of Geneva*. Article 4.2 further provides that confidential information may be disclosed only if explicit consent has been secured or if applicable law explicitly so provides. The *WHO Declaration* then goes on to specify, in Article 4.3, that "all identifiable patient data must be protected," and that such protection must be "appropriate to the manner of their storage." Also among its relevant provisions, Article 3.10, like the WMA *Declaration of Helsinki*, provides for consent and "proper ethics review" as general prerequisites for the conduct of scientific research.

3. *UNESCO Declaration on the Human Genome (1997)*

Founded in 1945, the United Nations Educational, Scientific and Cultural Organization (UNESCO) is a specialized agency of the United Nations. It includes within its mandate a mission to advance educational, scientific and cultural relations of the peoples of the world, as part of the greater UN commitment to the promotion of human dignity. Over the last decade, the pace of scientific developments and the impact of technology on modern culture, particularly as they affect evolving notions of human well-being, have not escaped the attention of UNESCO. Indeed, through the 1990s, UNESCO devoted increasing interdisciplinary attention, analysis and debate to a range of issues in such domains as genetics and society. The deliberations on genetics yielded, in 1997, the *Universal Declaration on the Human Genome and Human Rights (UNESCO Declaration)*.[32] Inspired in part by the *Universal Declaration on Human Rights* of 1948, the *UNESCO Declaration* offers to the world community a non-binding statement of principles and standards on the research, development and application of modern knowledge about genetics. Among its broad range of principles, some address the importance of research while others aim to ensure adequate data protection.

Article 12 of the *UNESCO Declaration* calls for the benefits from the human genome to be made available to all. The Article also deems "freedom of research" as part of freedom of thought. Though regarded as a freedom, research must still adhere to basic standards. Article 5 thus calls for rigorous risk–benefit assessments, prospective review of genome research protocols under national or international standards, and the free and informed consent of the individual or authorization by a substitute decision-maker for participation in research as prescribed by law.

The *UNESCO Declaration* further addresses personally identifiable genetic information. Indeed, it outlines a general duty of confidentiality of genetic data, subject to narrow exceptions. Article 7 provides as follows: "Genetic data associated with an identifiable person and stored or processed for the purposes of research or any other purpose must be held confidential in the conditions of law." (The *UNESCO Declaration* does not define "genetic data.") Article 9 further

[32] United Nations Educational, Scientific and Cultural Organization. *Universal Declaration on the Human Genome and Human Rights*. Paris, 1997. Online: http://www.unesco.org/ibc/en/genome/projet

stipulates that exceptions to the general principle of confidentiality must be based on "compelling reasons within the bounds of public international law and the international law of human rights." The formulation parallels the necessity standard for limiting infringements of privacy under the *Universal Declaration* and the ECHR, as noted in sections III.B and C, above. The *UNESCO Declaration* calls for the undertaking of measures to promote implementation of its principles. Accordingly, UNESCO's International Bioethics Committee has recently begun closer examination of the governing principles for privacy and confidentiality of genetic data.[33]

[33] See, for example, UNESCO, Working Group of the International Bioethics Committee on Confidentiality and Genetic Data. *Report on Confidentiality and Genetic Data*. Paris, June 2000.

IV. Selected National Data Protection Laws

Against the background of the foregoing international overview, this section profiles the national data protection law of selected nations. General principles of the leading national laws are introduced, followed by their particular provisions regarding health research. The laws are discussed consistent with the general methodology outlined in the Introduction, above.

A. Australia

The major source of national privacy protection in Australia is the federal *Privacy Act 1988*.[34] Because representatives from Australia presided over the working committee that developed the data protection standards for the 1981 *OECD Guidelines*, it is not surprising that the Act adopts and incorporates all *OECD Guidelines*. For years, the *Privacy Act* has applied to the federal public sector. As a result of the recently enacted *Privacy Amendment (Private Sector) Act 2000*,[35] however, the revision of the *Privacy Act (Revised Privacy Act*) has yielded legislation with a broader reach. Effective December 2001, the Revised Privacy Act extends personal information privacy standards to the private sector.

As in other countries that have recently revised their national data protection laws, Australia's *Revised Privacy Act* reflects an effort to give legal effect to the commitment of protecting privacy as a human right. Australia has manifested such commitment by signing and ratifying the *International Covenant on Civil and Political Rights (*CCPR), which recognizes privacy as a fundamental human right in public international law. (See Section II.D, above). Indeed, the CCPR is even mentioned in the Preamble to the *Privacy Act 1988*. The *Revised Privacy Act* also reflects how other pressing societal interests, such as health research, may compete with or even require limited incursions into privacy to advance the public interest.

The following section highlights: (1) the general provisions of the *Revised Privacy Act*, 2) a comparison of the established public-sector privacy principles and the new private-sector principles, and (3) the privacy guidelines for medical research issued or approved by the Privacy Commissioner under the *Revised Privacy Act*. Indeed, one of the noteworthy dimensions of the *Revised Privacy Act* is how it authorizes the Australian Privacy Commissioner to approve guidelines regarding the use of personal information in medical research, as developed under the Ministry of Health.

1. *The Privacy Act 1988*

The recently *Revised Privacy Act* has broader scope and more provisions for health research. The Privacy Commissioner of Australia oversees its implementation and enforcement.

---

[34] Commonwealth of Australia. *Privacy Act 1988.* Act No.119 of 1988, as amended. Online: www.austlii.edu.au

[35] Commonwealth of Australia. *Privacy Amendment (Private Sector) Act 2000*. Act No.155 of 2000, amending the *Privacy Act 1988.* Online: www.privacy.gov.au

As a result of the *Revised Privacy Act*, the public and private sectors are governed by a parallel set of privacy principles aimed at establishing co-regulatory national privacy protection. The principles outline the general standards for the collection, use and disclosure of personal information.

The Public Sector Standards: Information Privacy Principles (IPPs) and *The Private Sector: National Privacy Principles* (NPPs) are referred to in subsections d to f., below. Note that each of those items is described twice: for the IPPs and again for the NPPs.

Section 16 of the *Revised Privacy Act* obliges private-sector organizations to comply with NPPs or privacy codes approved by the Privacy Commissioner of Australia. As of spring 2001, no such codes had been approved. Nor had the Privacy Commissioner yet approved, under Section 95A, *Guidelines for National Privacy Principles on Health Information* for the private sector, as has been done for the public sector. Even with the approval of such codes or guidelines, the 10 NPPs, outlined in Schedule 3 of the *Revised Privacy Act*, will continue to define the general privacy standards for the private sector. They echo the basic principles adopted by the OECD in 1981, and parallel the longstanding IPPs for the public sector.

a. Scope

Australia's *Revised Privacy Act* of 1988 applies to both manually and electronically processed personal information within the federally regulated public sector and the private sector. Its provisions and standards have long applied to federal government "agencies," which generally include Australian government ministries, departments, courts, and special bodies. Most of these provisions centre around a core set of public-sector privacy standards, the IPPs.

Effective December 2001, a parallel set of privacy standards shall take effect for private-sector "organizations." Section 6.D of the *Revised Privacy Act* defines private-sector "organizations" to include, among other things: individuals, corporate bodies, partnerships, unincorporated associations and trusts; businesses with a turnover of $3 million or more; not-for-profit organizations such as charitable organizations, sports clubs and unions; federal government contractors; health service providers that hold personal health information; organizations carrying on a business that collects or discloses personal information for a benefit, service or advantage; and organizations so designated by regulation. "Organization" does not generally include small businesses. The new parallel standards for private sector "organizations" are called the NPPs. Both sets of principles, those for the public as well as the private sector, are described below.

b. Definitions

The *Revised Privacy Act* defines terms relevant to health research involving personal information. Section 6 of the *Revised Privacy Act* outlines common definitions for the public and private sectors. These include such terms as personal information, sensitive information, health information, and medical research.

"Personal information" refers to "information or an opinion … about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." "Individual" is defined as "a natural person." As a result of the 2000 Amendment, the *Revised*

Privacy Act defines "health information" as encompassing information about an individual's health or a disability, a health service provided or to be provided, and personal information collected in relation to the provision of a health service or in connection with the donation of one's bodily parts, organs, or substances. The *Revised Privacy Act* also offers a broad definition of "health service." The definition does not refer to research, nor does the *Revised Privacy A*ct define "health research." Instead, it defines "medical research" by stating that that "includes epidemiological research."

It should be noted that, as will be discussed below, other terms relevant to health research are defined in the public-sector health-research guidelines that have been adopted under the *Revised Privacy Act*. These include such terms as "identified data," "potentially identifiable" data, and "de-identified" data.

c. Special Protections: Sensitive Data

The *Revised Privacy Act* incorporates the concept of sensitive data. It thus departs from the original *OECD Guidelines*, and parallels most of the other international data protection norms outlined in Section III, above. The term "sensitive information" is broadly defined in Section 6 of the *Revised Privacy Act* to include information about an individual's racial or ethic origin, political opinions, religious beliefs, sexual preferences or practices, or health information. Thus "health information," as defined above, is considered sensitive data. Sensitive data is subject to special privacy standards under the NPPs, which have recently been included in the *Revised Privacy Act* to govern the private sector. The NPPs impose a general prohibition on the collection of sensitive data, unless individual consent is obtained or particular exceptions apply. Though no sensitive data provisions have been explicitly adopted for the public sector, the health research guidelines for the public sector do address health information that is considered sensitive data.

d.1 Consent: Data Collection, Use and Disclosure (IPPs)

The standards governing data protection in the public sector are inspired in part by the *OECD Guidelines*. Among other things, the Informational Privacy Principles provide that the collection of information must be undertaken for a lawful purpose and that such collection must be "necessary" to fulfill that purpose (Principle 1). Data must generally be collected directly from the individual concerned, be relevant to the purpose of collection, and be undertaken with a broad range of information disclosed, using fair and lawful means that are not unreasonably intrusive on privacy (Principles 2 and 3).

Like the *OECD Guidelines*, the standards do not speak explicitly of consent for the collection of personal information. Rather, the consent for collection is likely implied by the principle that required collection directly from the person concerned (Principle 2). Principle 9 requires that personal information be used only for relevant purposes. It is not to be used for other purposes or disclosed unless the individual concerned has consented or unless other exceptions apply under a necessity standard. These include that the use or disclosure is "necessary" for law enforcement, or to lessen a serious and imminent threat to life or health, or is required or authorized by law (principles 10 and 11). Details on such exceptions are noted below, in Section e.1.

d.2 Consent: Data Collection, Use and Disclosure (NPPs)

Under the NPPs for the private sector, personal information must be*:*

- collected—only if necessary and by lawful, fair and respectful means—from the individual (Principle 1)
- limited generally in the scope of use and disclosure to the primary purpose for collection (Principle 2)
- processed in an accurate, timely and complete manner (Principle 3)
- stored and secured (Principle 4)
- processed through, and managed by, personal information policies of organizations (Principle 5)
- accessible to, and correctable by, the individual concerned (Principle 6)
- linked by unique identifiers only under limited circumstances (Principle 7)
- made anonymous, if practicable and lawful to do so at the option of the individual (Principle 8)
- transferred to foreign countries under restricted circumstances (Principle 9)
- if considered to be sensitive data, be collected only under strict, limited conditions (Principle 10).

These principles impose a general standard of consent for the collection, use and disclosure of health information. Three of the Principles illustrate how.

First, for general data, Principle 1 requires, among other things, that the information be collected directly from the individual, who needs to be made "aware of" the purposes, needs, legal justifications, and parameters of the data processing. This parallels the public-sector principle and the original *OECD Guidelines.* That Principle 1.2 generally requires individuals to be made aware of the "consequences of the individual's refusal to provide the information" suggests that it generally contemplates individual consent.

Second, Principle 10 imposes a stricter standard for the collection of health information and like sensitive data. In the absence of consent or particular exceptions, health information is not to be collected. Principle 10.2 also imposes a consent standard on secondary uses. It requires organizations to not use or disclose information for other than the primary purpose of the collection, unless consent or particular exceptions apply.

Third, Principle 9 provides that information may be transferred to other nations that may not have substantially equivalent privacy protection, among other things, if the data subject consents. This would amount to a waiver of ordinary protections.

e.1 Exceptions and Research (IPPs)

Beyond the foregoing exceptions, the IPPs do not outline explicit exceptions for medical research. Instead, the *Revised Privacy Act* delegates authority for developing standards to the National Health and Medical Research Council of Australia (NHMRC). Section 95 of the *Revised Privacy Act* provides that an act by a Commonwealth of Australia agency that might be a breach of an IPP shall not be regarded as such if done in accordance with NHMRC guidelines for medical research, which have been approved by the Privacy Commissioner. As will be

shown in Part 3, below, these guidelines outline narrow exceptions for non-consensual use and disclosure of identifiable medical data.

e.2 Exceptions and Research (NPPs)

The private-sector principles also outline important exceptions to the general requirement that health information be collected and used only with individual consent. They even outline specific exceptions for research.

The sensitive-data and secondary-use rules, for instance, authorize non-consensual data processing under limited conditions of necessity. NPP 10.1 authorizes an organization to collect sensitive data, such as health information, without consent if the information is, among other things, "required by law" or otherwise "necessary" for particular legal proceedings. Non-consensual collection is also authorized for urgencies, when "the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent to the collection or physically cannot communicate consent." Similarly, Principle 2 authorizes non-consensual secondary use of data for a variety of necessities under limited circumstances. Many of these exceptions parallel those outlined in the *EU Privacy Directive* discussed in Section III.C, above.

The sensitive-data and secondary-use standards of the NPPs also authorize non-consensual data processing specifically for health research. Health information may be collected for research purposes without consent if four particular conditions prevail. Principle 10.3 provides, first, that the collection of health information must be "necessary" for limited research purposes. Such purposes include public health research, statistical analysis for public safety, or research for monitoring a health service. Second, the collection of identifying health information must also be necessary to accomplish the research purpose. Third, it must be impracticable for the organization to seek the individual's consent ("impracticable" is not defined). Fourth, the information must also be collected under particular authorities. It must be collected as (a) "required by law," or (b) in accordance with guidelines approved by the Privacy Commissioner under Section 95A of the *Revised Privacy Act*, or (c) "in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organization." Before information collected under Principle 10.3 may be disclosed, Principle 10.4 further obliges organizations to take reasonable steps to permanently de-identify the information.

Once personal health information is collected, Principle 2.1(d) authorizes non-consensual use and disclosure when "necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety." Such research is conditioned on three requirements: (a) that seeking individual consent is impracticable (impracticable is not defined); (b) "the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A"; and (c) for disclosures, the organization "reasonably believes" that recipients of the disclosed information will not disclose it or related personal information. Of note is the need for the use and disclosure to be done in accordance with commissioner-approved NHMRC guidelines for the private sector. As indicated below, such guidelines are anticipated for 2001–2002.

f.1. Data Retention and Security (IPPs)

Principle 4 of the IPPs outlines data security duties. According to this principle, those who keep records of personal information must implement reasonable security measures to protect against unauthorized access, loss or misuse. In contrast to the principles for the private sector, the IPPs seem not to explicitly specify either a period or standard for data retention.

f.2. Data Retention and Security (NPPs)

Principle 4 of the NPPs outlines data security and retention duties for the private sector. It obliges organizations to take "reasonable steps" to ensure the security of personal information against such events as misuse, destruction or loss. It differs from the public-sector principles in that it requires organizations to destroy or permanently de-identify personal information that is no longer needed, either for the purposes for which it was collected or for other authorized uses. This data retention principle is supplemented by standards contained in medical research guidelines issued by the NHMRC and approved by the Privacy Commissioner.

2. Medical and Health-research Guidelines Under the *Privacy Act*

Sections 95 and 95A of the *Revised Privacy Act* provide that the Australian NHMRC may, with the approval of the Privacy Commissioner, issue guidelines for the protection of privacy in the conduct of "medical research" involving the use of personal information.

Guidelines will be approved only if "the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence" to the personal information privacy protections. Privacy guidelines for medical research in the public sector have been recently revised. Those for the private sector are under development and are expected in late 2001 or in 2002.

2A. Established Public-sector Guidance

The NHMRC has recently drafted, and the Australian Privacy Commissioner has recently approved, revised privacy guidelines for medical research in the federal public sector: *Guidelines Under Section 95 of the Privacy Act 1988*.[36]

a. Scope

The public-sector Guidelines apply both directly and indirectly. Where medical research involves the use of personal information by the federal public sector, the Guidelines apply directly and must be followed for the information to be lawfully used or disclosed. The Guidelines "provide a framework for the conduct of medical research using information held by Commonwealth [of Australia] agencies where identified information needs to be used without consent." The scope of the Guidelines is broadened, however, by their incorporation of some standards and processes from other federal health-research documents, such as the NHMRC's *National Statement on Ethical Conduct in Research Involving Humans* (1999).[37]

---

[36] Australia, National Health and Medical Research Council. *Guidelines Under Section 95 of the Privacy Act 1988*. Canberra, 2000. Online: http://www.health.gov.au/nhmrc/issues/researchethics.htm

[37] National Health and Medical Research Council of Australia. *National Statement on Ethical Conduct in Research Involving Humans*, NHMRC, 1999: Preamble and s.18.

The latter also cross-references and incorporates the Section 95 public-sector Guidelines into its standards. As a result, the Guidelines are given broad and indirect application. Indeed, because this NHMRC national ethical statement requires recipients of federal health research monies to abide by the Guidelines as part of national norms on health research ethics, the Guidelines affect a range of non-governmental health research professionals and institutions.

b. Definitions

Beyond incorporating definitions from the *Revised Privacy Act*, the public-sector Guidelines include a glossary of other definitions directly relevant to health research. For instance, although they incorporate the *Revised Privacy Act*'s definition of "personal information," the use of the term includes identifying information for both individuals and groups. The explicit reference to groups may prove directly relevant to public health, genetic or population research.

The public-sector Guidelines define other terms for health research, including "identified data," "potentially identifiable" data, and "de-identified data." Data "that allow the identification of a specific individual" are "identified data." Personal health information that has been coded is de-identified, but to the extent that it may be "re-identified" by decoding, it remains "potentially identifiable."

The Guidelines reproduce the reference to "medical research"[38] from the *Revised Privacy Act*, but further define "research" as involving "systematic investigation to establish facts, principles and knowledge."

c. Special Protections: Sensitive Data

The Guidelines themselves make no explicit reference to sensitive data. However, the *Revised Privacy Act* defines "sensitive information" as including health and medical information. Accordingly, within the meaning of the *Revised Privacy Act*, the Guidelines address themselves to the processing of one class of sensitive data in the federal public sector.

d. Consent: Data Collection, Use and Disclosure

The Section 95 public-sector Guidelines are generally targeted at the non-consensual use of personal information for medical research. When the exceptions do not apply, the basic standards involving data collection, use and disclosure under the IPPs of Section 14 of the *Revised Privacy Act* generally apply.

e. Exceptions and Research

To justify the release of personal information that would otherwise violate an IPP under the *Revised Privacy Act*, an agency must ensure that "the research on which the personal information is to be used has been approved by a Human Research Ethics Committee (HREC) for the particular purpose in accordance with the Guidelines." The Guidelines thus generally outline the process and standards under which institutional research ethics committees may grant an exception to, and thus waive, the general requirement of consent for the use and disclosure of

[38] "Medical research" includes epidemiological research.

identifying data for medical research in the public sector. They do so by imposing process duties on researchers and corresponding standards of evaluation on the HRECs. The substantive standard for evaluating a researcher's request derives from Section 95 of the *Revised Privacy Act*, which asks: does the public interest in the research outweigh to "a substantial degree" the public interest in protecting privacy through adherence to the requirements of the Principles?

The researchers' duties, then, are tailored to outlining relevant information and specifying the request to the HREC. Guideline 2 requires researchers to submit a written proposal to a HREC, outlining the research project, the specific uses to which the personal information will be put, reasons why identified or potentially identified rather than de-identified information is required, why individual consent cannot be obtained, the estimated time of retention of the personal information, and security standards for storage of the data. Where the research may entail a breach of the Principles, specific reference should be made to the IPP that may be violated and the reasons why the public interest in the research outweighs the public interest in protecting privacy.

In evaluating proposals for non-consensual medical research, the HREC must adhere to basic procedural and substantive requirements. Guideline 3.1 requires the HREC to ensure that it has sufficient information about, expertise in and understanding of the privacy issues. Guideline 3.2 obliges HRECs, in considering whether to approve the research, to consider, among other things, if any IPPs will be breached, whether the use of identifiable or potentially identifiable data is "necessary," whether it is reasonable for the research to proceed without individual consent, and whether the public interest in the research "outweighs to a substantial degree" the public interest in protection of personal information privacy. Guideline 3.3 outlines a range of factors to evaluate in weighing "these public interests," including likely medical research advances, benefits to individuals, and whether the project imposes minimal risk of harm to individual privacy interests.

f. Data Retention and Security

The Section 95 public-sector Guidelines require that basic security and retention standards be applied to personal information. For instance, the Guidelines require that data be preserved "at least as secure[ly] as" required by the standards outlined in the *Joint NHMRC/AVCC Statement and Guidelines on Research Practice (Joint NHMRC/AVCC Statement)*. That document requires, among other things, that data management generally comply with relevant privacy norms; that department or research units establish data retention, access and security procedures; that data be recorded in a durable and appropriately referenced form; and that data be held for a "sufficient time" for such purposes as reference following publication of results. In the latter instance, it recommends a range of 5 to 15 years' retention post-publication, depending on the kind of research. The *Joint NHMRC/AVCC Statement* also imposes a general professional responsibility on investigators to ensure "appropriate security" in data processing.

(The category "Other Noteworthy Provisions" is not described for *Guidelines Under Section 95 of the Privacy Act 1988*.)

2B. Developing Private-sector Privacy Guidance

The *Revised Privacy Act* outlines two sections that authorize Australia's federal Privacy Commissioner to issue or to approve guidelines for research involving the privacy sector. Similar to Section 95, Section 95A of the Act authorizes the Commissioner to approve guidelines issued by the NMHRC for health research. The NMHRC has yet to do so. In the meantime, the Privacy Commissioner has relied on another section of the *Revised Privacy Act*. Section 27 of the Act authorizes the Commissioner to make guidelines about the NPPs. Thus, in the spring of 2001, the Commissioner released a public consultation document on health-research guidelines for the private sector, under Section 27 of the *Revised Privacy Act*. The document, *Draft Health Privacy Guidelines*,[39] is intended to yield public deliberations and final guidelines in 2001–2002. When finalized, the guidelines will provide interpretive guidance for the general rules applied to private-sector health research, as well as further standards for the non-consensual collection, use and disclosure of identifying health information under NPPs 2 and 10, as described above.

B. France

Both national and international trends have helped shape the protection of privacy and the content of data protection law in France. In the 1950s, France signed the *ECHR*. As described in Section II.B, above, Article 8 of the Convention imposes a human rights obligation to respect private and family life. France has also been a member of the Organization for Economic Co-operation and Development since the early 1960s, and has adopted the *OECD Guidelines*. As a member of the Council of Europe, France signed and ratified, in the early 1980s, *COE Convention 108/1981*. As a member of the European Union, it has an obligation to harmonize its law with the *EU Privacy Directive*.

In the context of these international obligations, France has moved over the years to implement the respect of privacy and data protection norms in a variety of formal legal undertakings. Article 9 of the *Civil Code*[40] of France, for instance, proclaims that everyone has the right to respect of one's private life. The Constitutional Court of France has ruled that the right to privacy is implicit in the French Constitution.[41] Recent amendments to professional ethics codes have heightened ethical and legal duties of confidentiality. For instance, articles 4 and 72 of the *Code de Déontologie médicale*[42] indicate that physicians must ensure that those assisting the physician conform to a professional obligation of confidentiality that is enforced by provisions of the French *Penal Code*.[43] Over the last two decades, moreover, France has enacted data protection legislation and health research provisions that govern the use of personal information. Highlights of the data protection law follow.

---

39 Australia, Privacy Commissioner. *Draft Health Privacy Guidelines*. Canberra, 14 May 2001. Online: www.privacy.gov.au

40 *Code Civil.* Online: www.legifrance.gouv.fr/citoyen/new_code.ow

41 *Décision 94-352 du Conseil Constitutionnel du 18 janvier 1995*.

42 *Code de Déontologie médicale*. Online : www.legifrance.gouv.fr/citoyen/new_code.ow

43 *Code Pénal*. Online : www.legifrance.gouv.fr/citoyen/new_code.ow

1. *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Data Protection Act: Law 78-17) (1978)*

French data protection legislation dates at least from the late 1970s, when the Parliament enacted *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (*Law 78-17 Respecting Data Processing, Records and Freedoms)*.[44] Enacted before most modern international data protection norms discussed in Section III, above, *Law 78-17* has been amended several times. While other laws contain standards pertinent to personal information, *Law 78-17* today remains the central piece of legislation on the protection of personal data in France. It does so through its data protection standards and through oversight by the National Data Processing and Liberties Commission (CNIL).[45] As will be shown, recent amendments to the law have added data protection norms specifically for health research.

a. Scope

Law 78-17 generally addresses the collection, recording and storage of personal information. Initially, it applied to data processed by automated and computer systems, but amendments have expanded its application in recent years. Articles 45 and 46 now extend core provisions of the law to "non-computerized and mechanically processed records." The provisions also empower government to extend the law to particular sectors through regulatory decrees. Article 4 of *Law 78-17* indicates that it applies to public and private bodies. Even with these recently broadened parameters, it should be noted that, under Article 40-1, *Law 78-17* does not apply to data processed for medical treatment. Nor does it apply to the processing of data for research, if such processing is made in the course of medical treatment.

b. Definitions

Law 78-17 defines a few important terms. For example, Article 4 defines the term "nominative" as "permitting, directly or indirectly, the identification of physical persons through processing of data." Article 5 of the law refers to "automated" processing as "automated means used to collect, record, elaborate, modify, preserve or destroy nominative data." Though *Law 78-17* has been amended to incorporate provisions on health research, "research" is not explicitly defined.

c. Special Protections: Sensitive Data

Law 78-17 offers special protections for some classes of sensitive data. Article 31 of *Law 78-17* generally prohibits the collection or storage of identifying sensitive data without the express consent of the individual. Reference is made to information relating to an individual's racial origin, political, philosophical or religious opinions, or union affiliation. The list does not refer to information related to an individual's health, in contrast with the *EU Privacy Directive* and *COE Convention 108/1981*. (See Section III, above.) The omission is important because sensitive data is given particular protections, such as a general prohibition against its secondary use under Article 29 and a general prohibition against retaining such information in a computer without express consent under Article 31. Still, as elaborated below, 1994 amendments to the

[44] *Loi nº 78-17 du 6 janvier1978 relative à l'informatique, aux fichiers et aux libertés*. *Journal Officiel* du 7 janvier 1978, as amended. Online: www.legifrance.gouv.fr

[45] *La Commission nationale de l'informatique et des libertés de la France*. Online: www.cnil.fr

law introduced special provisions for health research involving personally identifiable health information.

d. Consent: Data Collection, Use and Disclosure

Some of *Law 78-17*'s provisions on data processing parallel those of the *OECD Guidelines* and some diverge from them—perhaps because *Law 78-17* pre-dates the *OECD Guidelines*. In 1994, however, *Law 78-17* underwent significant modification to address health research.[46] The amendment was further elaborated by *Decree 95-682 of 9 May 1995*.[47] Through the amendment, the French Parliament created specific provisions for the processing of personal information for health research within the general data protection law *78-17*. The revised standards and processes outline an approach that affects researchers, research subjects, administrative overview, and recipients of health research data.

Article 40-1 provides that researchers may generally process nominative information for health research, but qualifying conditions apply. As per Article 40-2, the researcher must submit his or her research proposal to an advisory committee on the treatment of information in research and health care. Committee review is to be based on the research methodology and the relevance of the required nominative data to the scientific objectives. Authorization is thereafter required by the National Data Processing and Liberties Commission (CNIL), the independent 17-member commission for implementing, overseeing and enforcing the data protection standards. The CNIL remains responsible for the proper treatment of nominative computerized data in accordance with the law. As part of the research design and implementation, Article 40-3 imposes a general duty to code identifying health data for transmission, unless particular exceptions apply. (See Section e., below.) When the results of the research are communicated, as in a publication, they must be anonymized. Recipients of such health data are, under Article 40-3, subject to an obligation of professional secrecy whose violation is punishable by penal sanctions. The obligations and standards regarding confidentiality, coding, transmission and secondary use of personal data have been reiterated and elaborated in recommendations by the CNIL.[48]

Law 78-17, as amended, outlines at least three instances when consent standards apply. First, consent applies to the preservation of sensitive data, as noted above in Section b. Second, the 1994 amendments specified consent standards and rights of informed opposition to data processing for health research. Article 40-4 provides for a general right of the individual to oppose the processing of nominative data for health research; Article 40-5 outlines a right to be informed, among other things, before the processing, of the purpose, nature, likely recipients, etc. of the information to be processed for health research. For research involving identifying biological samples, Article 40-4 requires informed and express consent. For the processing of information regarding the deceased, Article 40-4 authorizes it unless the person, while alive, had expressed

---

46 *Loi nº 94-548 du 1 juillet 1994* relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal Officiel* du 2 juillet 1994.

47 *Décret nº 95-682 du 9 mai 1995. Journal Officiel* du 11 mai 1995, art. 40-3, al. 2.

48 See, e.g., La Commission nationale de l'informatique et des libertés. Délibération nº 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. *Journal Officiel* du 12 avril 1997.

written opposition to such use. Third, consent standards also apply to the secondary use of data. Article 28 generally prohibits the non-consensual use of data beyond the original purpose for which it was collected, unless certain exceptions apply. (See Section e., below.)

e. Exceptions and Research

Existing standards for the processing of nominative personal information outline at least three important exceptions regarding health research. First, Article 40-3 authorizes an exception to the general duty to code identifying health data for transmission, when identification is necessary for the particular pharmacological studies, if research protocols require identification, or if required for special collaborative national or international research. Second, Article 40-5 may authorize non-consensual secondary uses of collected data, depending on the difficulty in contacting the individuals concerned for consent. Third, Article 28 authorizes non-consensual data retention for "historical, statistical and scientific research" purposes.[49] Such retention must further conform to the requirements of the *Law Respecting Archives*.[50]

f. Data Security and Retention

Articles 28 and 29 outline minimal duties regarding the security measures and length of data retention. Article 28 outlines a general standard that information not be kept in nominative form beyond the time required to achieve the goals for which it was collected or processed. As noted, Article 28 provides an exception to this for information retained for "historical, statistical or scientific purposes." Article 29 imposes a general duty of care to undertake reasonable security precautions to prevent unauthorized access, disclosure or destruction. To complement these provisions, the CNIL has recommended the encryption or scrambling of information where data systems involve ongoing follow-up and updating.[51] Heightened security measures adopted for medical data are also subject to verification by the CNIL.

g. Other Noteworthy Provisions

Law 78-17 also outlines a number of provisions to ensure implementation of privacy protection. Three examples illustrate the range of provisions.

First, for international research collaboration, Article 40-9 provides that nominative health data may not be transferred to a receiving country that does not offer similar protection of personal data. This parallels the *EU Privacy Directive*.

Second, articles 6 to 33 outline the creation and responsibilities of the CNIL. Some of the Commission's roles have been noted above. Its general regulatory responsibilities include authorizing public institutions to process particular data, registering and overseeing private-sector data processing, issuing simplified standards, providing advice on data processing,

---

49 Compare Article 8 of the *EU Privacy Directive* and Article 9 of *COE Convention 108/1988* in Section III, above.

50 *Loi n° 79-18 du 3 janvier 1979 relative aux archives*, art.4-1. *Journal Officiel* du 5 janvier 1979:49; corrected in *Journal Officiel* du 6 janvier 1979:55. Online: www.cnil.fr/textes/text052.htm

51 La Commission nationale de l'informatique et des libertés. Délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. *Journal Officiel* du12 avril 1997.

investigating written privacy complaints, and advising government[52] on legal reforms for data protection.

Third, French society has invoked criminal law powers to advance the protection of personal privacy with respect to the automated processing of nominative data. Such provisions are found in both *Law 78-17* itself and the *Penal Code*, as amended 16 December 1992. Penal sanctions may be imposed for such matters as unlawful or fraudulent data processing, violation of information security, non-consensual retention of data, retention of data beyond the prescribed period, unauthorized use, or unlawful disclosures. Such provisions may help explain why French law has been regarded[53] as an example of a system that strictly protects privacy and medical confidentiality.

2. Implementation of the *EU Privacy Directive: Loi sur la Société de l'Information*

Like many members of the European Union, France has recently undertaken formal legal initiatives to incorporate the *EU Privacy Directive* into national law.[54] Toward this end, the French Parliament is actively considering new legislation, the *Loi sur la Société de l'Information*. This law has been proposed to amend *Law 78-17*, the existing data protection legislation. The proposed provisions include, among others, (a) broadening of the scope of certain fundamental rights, (b) simplification of standards, (c) strengthening of the powers and resources of the CNIL, and (d) harmonization of data processing standards between the public and private sectors.[55] The legislation is expected to be adopted in 2001–2002.

C. The Netherlands

The evolution of data protection law in the Netherlands reflects that country's international legal obligations and its national commitments to protecting individual privacy. In the 1950s, the Netherlands signed and ratified the ECHR. As noted in Section III, above, the Convention recognizes the respect for human privacy as a fundamental human right, subject to reasonable democratic necessities that may sometimes require infringements on privacy. As a member of the Organization for Economic Co-operation and Development (OECD) since the early 1960s, the Netherlands has had formal occasion to consider and implement the *OECD Guidelines*. As a member of the European Union, the Netherlands is obliged to harmonize national legislation with the *EU Privacy Directive*.

The legal obligations that flow from such international relations would seem to have manifested themselves in at least two formal legal initiatives in the Netherlands over the last 15 years. The

---

52 *Décret nº 78-774, du 17 juillet 1977. Journal Officiel* du 23 juillet 1997, art. 20, 3Eº.

53 Mason J.K., McCall Smith R.A. *Law and Medical Ethics*. 4th ed. Butterworth's: London, 1994: 169.

54 Braibant G. *Données Personnelles et Société de l'Information : Rapport au Premier Ministre sur la transposition en droit français de la directive nº 95/46.* Paris, 3 mars 1998. Online: www.cnil.fr/textes/indextranspo.htm

55 Online: www.internet.gouv.fr

Netherlands is, for instance, one of the few nations sampled in this survey whose Constitution explicitly protects privacy. What is more, that constitutional privacy protection explicitly requires that "rules to protect privacy" shall be laid down by Act of Parliament "in connection with the recording and dissemination of personal data."[56] Responding to this constitutional requirement, the Netherlands Parliament enacted omnibus data protection legislation in 1988.[57] Over a decade later, a new data protection law was adopted. Highlights of the new legislation follow.

1. *Wet bescherming persoonsgegevens (Personal Data Protection Act) (2000)*

In July 2000, Parliament approved the *Wet bescherming persoonsgegevens (Personal Data Protection Act)* (PDPA).[58] This updates and supersedes the original data protection law of 1988, in a move toward implementing the *EU Privacy Directive*. The Data Protection Commission oversees the administration and implementation of its provisions.

a. Scope

Article 2 of the Act outlines its scope. The Act applies to personal data processed by automated, partly automated, or non-automated systems entered or intended to be entered in a file. It generally applies to data processing in the public and private sectors of the Netherlands, and to those outside the EU that use data processing means situated in the Netherlands.

b. Definitions

The Act provides definitions for several terms, including "personal data," "processing" and "consent." "Personal data" is defined as information "relating to an identified or identifiable natural person." The definition does not define "identifying." The Act broadly defines "processing" as including the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination, merging, linking, and erasure or destruction of data.

c. Special Protections: Sensitive Data

The PDPA outlines heightened protections for special categories of personal data, including health information. Article 16 imposes a general prohibition against processing personal data concerning, among other things: religion; race; political convictions; criminal, unlawful or objectionable behaviour; health; and sexual life. Article 23 provides exceptions to the prohibition on diverse grounds, including the express consent of the data subject; or when "necessary" for particular legal proceedings or to advance "important public interests," with appropriate privacy protection provided for by law or by an exemption of the Data Protection Commission. Other exceptions relevant to health research are outlined below.

---

56 *Constitution of the Kingdom of the Netherlands* 1989, art.10.

57 *Wet persoonsregistraties (Law on Registration of Personal Data)*. 28 December 1988. The Dutch Data Registration Act, 1988. Online: http://home.planet.nl/~privacy1 See also Ploem M.C. Medical Research and Informational Privacy. *Medicine and Law* 1998;17:287-297.

58 *Wet bescherming persoonsgegevens (Personal Data Protection Act)*. 6 July 2000. Staatsblad 2000 302 (unofficial translation). Online: http://www.registratiekamer.nl; http://home.planet.nl/~privacy1

d. Consent: Data Collection, Use and Disclosure

The PDPA reflects many of the general data processing standards of the original *OECD Guidelines*, as modified by the *EU Privacy Directive*. Article 7 of the Act mirrors Article 6(b) of the *EU Privacy Directive* by providing that the collection of personal data must be for "specific, explicitly defined and legitimate purposes." Article 9 complements this general requirement by precluding further processing "in a way incompatible with the purposes for which they have been obtained." It then outlines a series of factors to evaluate whether further processing is ''incompatible." As noted below, further processing for "scientific purposes" will not be regarded as incompatible under particular conditions.

Article 8 outlines a core standard governing the processing of data: the general requirement for the data subject's "unambiguous" consent. Consent is defined in Article 1 as involving a "freely given, specific and informed" agreement to processing of personal data. Article 23, as noted above, provides for an exception to the prohibition on the processing of personal data if done with the "express consent" of the data subject.

e. Exceptions and Research

The PDPA also outlines some non-consensual data processing for health and scientific research. Four examples illustrate how.

First, Article 21 provides that the general prohibition on non-consensual processing of personal health data does not apply where the processing is carried out by medical professionals or health care institutions if "necessary" for the care and treatment of the data subject, or for the administration of the institution or professional practice concerned.

Second, Article 34(4) relieves institutions of the requirement to provide data subject information when to do so "appears to be impossible or would involve a disproportionate effort." In such circumstances, Article 44 indicates data processing will not be subject to particular informational disclosures.

Third, Article 9 of the PDPA provides an explicit exception to the general prohibition against non-consensual or unauthorized "incompatible uses" of collected personal data. Further processing of personal data is deemed not an "incompatible purpose," however, if done for "historical, statistical or scientific purposes." Arrangements must be made to ensure that such further processing is restricted to those limited purposes. The exception under Article 9 has further conditions. Article 9 specifies that processing "shall not take place where precluded by an obligation of confidentiality by virtue of … profession or legal provision." Since the *Wet geneeskundige behandelingsovereenkomst (Medical Treatment Contract Act)*[59] outlines specific obligations of confidentiality for physicians involved in medical treatment, its provisions may also govern some uses of patient data in research. For instance, it similarly authorizes, in strictly limited circumstances, non-consensual access to health information for statistical and scientific research involving public health.

---

[59] *Wet geneeskundige behandelingsovereenkomst (Medical Treatment Contract Act)*. 17 November 1994. Stb 1994. Article 458 authorizes access if, among other things, (a) consent cannot be reasonably requested and guarantees are provided that privacy will not be inordinately infringed, (b) the research is in the public interest and cannot be conducted without the information, and (c) the patient has not specifically objected to the information being provided.

Fourth, Article 23 outlines a narrow exception to the general requirement of consent for the processing of personal data concerning health for purposes of "scientific research or statistics." The following conditions must apply: (a) the research must serve a public interest, (b) the processing must be "necessary" for conducting the research or gathering the statistics, (c) express consent must be either "impossible" or involve a "disproportionate effort," and (d) sufficient guarantees need to be provided to ensure that the processing "does not adversely affect the individual privacy of the data subject to a disproportionate extent." Article 21(4) outlines similar restrictive criteria for scientific and statistical research concerning personal genetic data for which the researcher does not have the express consent of the data subject.

f. Data Security and Retention

The PDPA also outlines general data security and retention duties. Article 10, consistent with the original *OECD Guidelines*, generally provides that personal data shall not be kept for any longer than is necessary for achieving the purposes for which it was collected or subsequently processed. As noted above, the standard is subject to an exception for "historical, statistical or scientific purposes," where the responsible party has made the necessary arrangements to ensure that the data concerned are used solely for these specific purposes. Articles 12 to 14 impose a general duty of confidentiality for processors of personal data, and further require the implementation of "appropriate" technical organization and security measures against loss, destruction, and unnecessary or unlawful data processing.

g. Other Noteworthy Provisions

Several provisions of the PDPA are intended to advance its implementation consistent with the *EU Privacy Directive* and the societal needs of the Netherlands. The Act, for instance, created the Data Protection Commission to administer and oversee implementation of its provisions. The Commission is authorized to, among other things, advise on data protection law reforms, investigate complaints of privacy violations, and oversee compliance with the PDPA. Such responsibilities address the requirement under the *EU Privacy Directive* for an independent supervisory authority to oversee national data protection principles.

Two other provisions relating to the Commission's broader duties are noteworthy. First, under Article 25 of the Act, the Commission has the authority to approve codes of conduct that it deems consistent with the principles and legal provisions of the PDPA. Such codes of conduct may be undertaken by organizations for different sectors of society and submitted to the Commission. Second, articles 51 and 52 give the Commission a role to oversee the processing of personal data where the processing takes place in accordance with the laws of another country of the European Union. Under Article 76, personal data generally shall not be transferred outside the European Union unless the receiving country guarantees an "adequate" level of protection. An assessment of the adequacy of the level of protection shall take account of the circumstances affecting a data transfer operation or a category of data transfer operations. Account shall be taken in particular of the type of data, the purpose or purposes and the duration of the planned processing or processing operations, the country of origin and country of final destination, and the general and sectoral legal provisions applying in the non-member country concerned, as well as the rules governing the business sector and security rules applying in these countries.

D. New Zealand

As a member of the Organization for Economic Co-operation and Development since the 1970s, New Zealand has had formal occasion to review and consider adopting the *OECD Guidelines*. As one of many nations to have signed and ratified the CCPR, New Zealand has manifested formal international commitment to respect for human rights, including privacy. Consistent with both of these traditions as they bear on health research, New Zealand undertook major data protection initiatives in the 1990s.

In 1993, New Zealand enacted national data protection legislation in the form of a *Privacy Act*. A year later, it adopted its *Health Information Privacy Code* (HIPC). Highlights of both follow. Because there are many parallel and even identical standards in the two documents, more extensive discussion of identical standards is sometimes deferred to the analysis of the *Health Information Privacy Code*.

1. *The Privacy Act (1993)*

Overseen by an independent commissioner of privacy, the *Privacy Act 1993*[60] of New Zealand is an omnibus data protection law whose central purpose is to set statutory controls on how public and private entities collect, use and disclose personal information. The Act is based on the 1980 *OECD Guidelines* and the IPPs of the *Privacy Act 1988* of Australia.[61] Due in part to standard review of national legislation and in part to the need to harmonize the Act with newer international norms, such as those outlined in the *EU Privacy Directive*, there have been ongoing deliberations in recent years about the merits of amending particular provisions of the Act.

a. Scope

The Act covers all "personal information" as defined below. This includes automatically processed data in both the private and public sectors.

b. Definitions

Section 2 defines several concepts central to the working of the Act. For example, "personal information"[62] is defined as "information about an identifiable individual; and includes information contained in any register of deaths …." "Individual'' is further defined as a natural living person, meaning that the Act generally applies to personal information about those alive. There are exceptions to this rule. Section 46(6) indicates that for the purposes of a code of practice relating to health information, personal information includes that relating to living or deceased individuals. Codes of practice are explained below. The Act does not directly define "health information," but it refers indirectly to the definition outlined in other New Zealand legislation.[63] The Act also indicates that it applies to "agencies." These are generally defined as any person or body of persons, whether corporate or unincorporated, in the public or private sector.

---

60 *Privacy Act 1993*. Online: www.privacy.org.nz/recept/rectop.html

61 Basinar D. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. Epic: 2000:162.

62 *Re Application by L* (1997) 3 HNRX 716 (Complaints Review Tribunal) has held that personal information can include mentally processed information.

63 Section 22B of the *Health Act 1956.*

c. Special Protections: Sensitive Data

New Zealand's *Privacy Act* does not expressly include special provisions for "sensitive data." It has thus followed the original 1981 *OECD Guidelines*. However, in the HIPC, adopted under the *Privacy Act*, particular provisions are outlined for the processing of identifiable health information. (This is discussed below.) Moreover, the merits of expressly including sensitive data protections have recently been aired in public analyses and discussion of revisions to the *Privacy Act*.[64]

d. Consent: Data Collection, Use and Disclosure

Section 6 of the *Privacy Act* outlines 12 *Privacy Information Principles* that define core standards under the Act. These echo the principles adopted by the OECD in 1981. (See Section III, above). Under the principles, personal information must be:

- collected for lawful and necessary purposes (Principle 1)
- collected directly from the individual (Principle 2)
- collected such that individuals are informed of the data processing (Principle 3)
- collected in a lawful, fair and reasonable manner (Principle 4)
- stored and secured (Principle 5)
- accessible by the individual concerned (Principle 6)
- correctable by the individual concerned (Principle 7)
- verified for accuracy before use (Principle 8)
- kept for a reasonable period of time (Principle 9)
- limited in scope of use (Principle 10)
- disclosed only under limited circumstances (Principle 11)
- linked by unique identifiers only under limited circumstances (Principle 12).

The consent or "authorization" provisions of the *Privacy Act* are largely identical to those of the HIPC. As such, provisions of the latter are discussed below in the analysis of the Code.

e. Exceptions and Research

The general requirement governing the collection, use and disclosure of personal information is exceptionally set aside for information that is publicly available, when compliance is judged impracticable, when the data are non-identifying, or when the use of personal data is deemed "necessary" for legal proceedings, law enforcement, or for avoiding imminent harms or prejudice to physical or mental health.

There are also specific provisions for research. Because these are largely identical to those outlined in the HIPC, the provisions of the latter are discussed below.

Also, more generally, Section 54 of the Act provides that agencies may be authorized by the Commissioner to collect or use personal information sometimes in breach of principles governing the collection (Principle 2), use (Principle 10), and disclosure (Principle 11) of information. To

[64] Privacy Commissioner of New Zealand. *Discussion Paper No. 12: New Privacy Protections*. Auckland, 1998. Online: www.privacy.org.nz/slegisf.html

obtain such authorization, the Commissioner must find that any interference with the individual's privacy is justified and outweighed by a substantial public interest or by a clear benefit to the individual.

f. Data Retention and Security

Principles 5 and 9 largely reflect the *OECD Guidelines* on data retention and security, as discussed in Section III, above. They are also, for the most part, identical to the data security and retention duties imposed under the HIPC. Accordingly, provisions of the latter are discussed below.

g. Other Noteworthy Provisions

The *Privacy Act* outlines a number of provisions for practical implementation of privacy principles and standards. At least two are particularly relevant for health research.

One concerns implementation and oversight by an independent supervisory body, the Privacy Commissioner of New Zealand. The Commissioner's principal functions include: promoting the principles of the Act and examining proposed legislation and governmental policies that may affect the privacy of individuals; reviewing the operation of the Act, monitoring the use of unique identifiers, and approving exemptions from the information privacy principles; and receiving, investigating and conciliating complaints. The second noteworthy provision concerns particular regulatory powers of the Commissioner. The Commissioner may issue codes of practice that elaborate or modify standards of the Act. As is explained below, the Commissioner has done so for health information.

2. *The Health Information Privacy Code* (HIPC) (1994)

Section 46 of the New Zealand *Privacy Act* empowers the Privacy Commissioner of New Zealand to issue codes of practice that take into account the special characteristics of specific industries, agencies or types of personal information. Section 46 specifically indicates that such codes of practice may modify the application of the *Information Privacy Principles* of the *Privacy Act*. They may even prescribe standards that are more or less stringent than the principles. To issue a code of practice, the Privacy Commissioner is obliged to give broad public notice of his or her intent to do so, to consult with affected interests, and to submit the code to the New Zealand Parliament for deliberations before the code takes effect. Once in effect, a code has the force of law. Acting under this authority and process, the Commissioner issued the New Zealand *Health Information Privacy Code* (HIPC) in 1994.[65] It has been revised as recently as the year 2000. As will be shown, the language, privacy standards and exceptions in the HIPC have been specifically tailored to the health sector.

a. Scope

The HIPC regulates the collection, use and disclosure of identifiable health information by public and private agencies. It thus applies to health service providers, health professional

[65] Privacy Commissioner of New Zealand. *Health Information Privacy Code*, as amended, Auckland, 1994; revised edition, 2000. Online: www.privacy.org.nz/recept/rectop.html

schools, selected government health agencies, health professional bodies, and manufacturers and vendors of medicines and medical devices.

b. Definitions

Section 4 of the HIPC outlines a broad definition of identifiable "health information," which includes information about an individual's health, medical history, disabilities, bodily substance tests, and health services received.

c. Special Protections: Sensitive Data

Like the *Privacy Act* of New Zealand, the HIPC does not explicitly refer to identifiable health information as "sensitive data" warranting special protections.

d. Consent: Data Collection, Use and Disclosure

HIPC provides that the collection of information must be undertaken for a lawful purpose and that such collection must be "necessary" to fulfill that purpose. Rule 2 generally requires that health information be collected "directly from the individual concerned." Rule 3 generally obliges agencies collecting data to take reasonable steps to ensure that the individual "is aware" of, among other things, the purpose and intended recipients of the data, as well as "whether or not the supply of the information is voluntary or mandatory." The HIPC also imposes a general standard to help to protect individual privacy regarding unique identifiers. Rule 12 provides that individuals are not to be assigned a unique identifier unless it is "necessary to enable the health agency to carry out" its functions efficiently.

It should be noted that the HIPC does not use the term "consent" as a standard for the collection, use or disclosure of health information. Instead, it uses the word "authorization." Thus, rules 10 and 11 condition the "disclosure" and "use" of personally identifiable health information on a general requirement that the "authorization" of the individual or his or her representative be secured. The term "authorization" is not defined.

e. Exceptions and Research

The HIPC outlines a number of exceptions to the general requirements for processing identifiable personal health information. They apply to the collection, use and disclosure standards. For instance, Rule 3(4) provides that the general obligation to collect personal health data directly from the individual is not required if the agency "reasonably believes" that compliance would "prejudice the purposes of collection" or is not "reasonably practicable." "Practicable" is not defined.

Rules 10 and 11 provide exceptions specifically relevant to health research. They allow for non-consensual use and disclosure under particular standards. For instance, under rule 10(1)(e), neither consent nor necessity is required for the "use" of personal identifying information if the agency "reasonably believes" that the health information is non-identifying, is used for statistical purposes in a non-identifying manner, or is used under particular conditions for "research purposes." Those "research purpose" conditions generally require that a research ethics committee approve the use and that the data "not be published in a form that could reasonably be expected to identify the individual concerned."

Rule 11(2)(c) outlines similar "research purpose" criteria for non-consensual disclosure of health data. This rule applies if there are reasonable grounds to believe that "it is either not desirable or not practicable to obtain authorisation." When such non-consensual disclosure is justified, Rule 11 still imposes a limitation. It provides that disclosure is permitted "only to the extent necessary for the particular purpose." The limitation is consistent with the narrow-exceptions approach outlined in the original *OECD Guidelines* and expanded in such documents as the *EU Privacy Directive*.

f. Data Retention and Security

Rules 5 and 9 of the HIPC outline data retention and security duties. Rule 5 imposes a duty to protect health information "by such security safeguards as is reasonable in the circumstances" to prevent such events as loss, misuse or unauthorized disclosure. It also imposes a duty to dispose of documents in a manner that preserves the privacy of the individual. Rule 9 requires that information be kept for no longer than is required for the purposes for which it is to be lawfully used. Both rules are consistent with the data security and retention principles of the original *OECD Guidelines*. (See Section III, above.) It should also be noted that if health information about an identifiable individual is held by a health professional, then data retention standards of other New Zealand health laws may apply. Regulations adopted under some such laws, for instance, may require health agencies to retain health information for a minimum of 10 years.[66]

(The category "Other Noteworthy Provisions" is not described for the HIPC.)

E. United Kingdom

Particularly in recent years, the formal relations that the United Kingdom (UK) enjoys in the international community have helped to generate legal changes that have begun to influence health research. Indeed, some of these international relationships and their associated European legal obligations have exerted a direct and significant influence on recent privacy and data protection laws of the UK. They have done so in at least three respects.

First, as a member state of the Council of Europe for decades, the UK signed and ratified the ECHR in the 1950s and *COE Convention 108/1981* in the 1980s. Both treaties are discussed in Section II, above.

The UK's obligations under the ECHR have recently contributed to its adoption of a *Human Rights Act* for the UK.[67] The *Human Rights Act* adopts verbatim Article 8 of the ECHR into UK law, thus making more explicit in British society the "right to respect private life," subject to limitations in accordance with law as "are necessary in a democratic society …."

---

66 See *Health (Retention of Health Information) Regulations 1996*, adopted under the *Health Act 1956*.

67 United Kingdom. *Human Rights Act* 1998, c. 42.

Second, the UK's membership since the 1960s in the Organization for Economic Co-operation and Development has meant that it formally has had opportunity to consider and move toward implementation of the *OECD Guidelines*. As will be shown below, the UK has done so in part through national data protection initiatives, such as the original data protection legislation of 1984.

Third, for decades the UK has been a member state of the European Economic Community/European Union, meaning that the country is obliged to incorporate the principles of the *EU Privacy Directive* into national data protection practices. It has done so in part by revising its original data protection law by means of a new *Data Protection Act* of 1998 (DPA). That initiative, in turn, has helped to prompt some governmental research and health professional organizations to update and issue revised ethical guidelines on health research. Highlights of the revised DPA and the revised guidelines of the Medical Research Council and British Medical Association follow.

1. *Data Protection Act (DPA) (1998)*

Enacted in July 1998 to take effect in March 2000, the *Data Protection Act*[68] (DPA) of 1998 updates previous UK data protection law to bring it into accordance with the requirements of the *EU Privacy Directive*. The DPA is supervised by the Data Protection Commissioner.

a. Scope

The DPA applies to personal data: that is, data about identifiable living individuals, processed in either the public or private sector of the United Kingdom. As such (and in contrast to the United Nations standards), the Act does not cover information about the deceased. Under the definition of personal data outlined below, data that have previously been anonymized are also outside the scope of the DPA.

b. Definitions

The Act specifies definitions for several terms, including "personal data," "processing," and "sensitive data." "Personal data," defined in Section 1, refers to personal identifying information about a living individual. Such identifying information may come either directly from the data in question or indirectly—that is, when the data in question are, or are likely to be, combined with other information. This is a broad definition of "identifiable."

Section 1 also broadly defines data "processing" to mean "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including … adaptation or alteration, … retrieval, consultation or use, … disclosure … or … erasure or destruction of the information or data … ." "Sensitive data" is defined as "including all information about physical or mental health or condition, or sexual life."

[68] United Kingdom. *Data Protection Act 1998, c*. 29, superseding the *Data Protection Act* of 1984. Online: www.dataprotection.gov.uk

c. Special Protections: Sensitive Data

The DPA provides special provisions for such sensitive data as identifiable health information.

"Sensitive data," according to Section 2, encompasses information relating to one's "physical or mental health or condition."

Schedule 3 of the Act then provides that sensitive data must be processed under particular conditions. Those conditions generally require either the "explicit consent" of the individual or a demonstration that non-consensual processing is "necessary"; for example: (a) for employment responsibilities, as required by law; or (b) in particular circumstances, to protect the vital interests of the data subject or another; or (c) for administration of justice purposes or legal proceedings; or (d) for "medical purposes" that include care, prevention, diagnosis and medical research. When processing is required for medical purposes, it must be done by either a health professional or a person who has an equivalent duty of confidentiality.

Schedule 3 provides some policy flexibility by specifically enabling government to outline other non-enumerated conditions for research involving sensitive personal data. The government chose to do so in 2000 by means of *Statutory Instrument 2000 No. 417*. This addresses data processing for some "research purposes" that would include maintaining statistical or research archives.[69] Such research may be done if the processing is "in the substantial public interest," is "necessary for research purposes," is unlikely to cause "substantial damage or distress," and does not implicate or support measures about a particular data subject. Even with such elaborations, some analysts are calling for detailed definitions and further refinements of DPA standards so as to more precisely guide health research for consensual, non-consensual and anonymized circumstances in the UK.[70]

It should be noted that although the sensitive data provisions in the DPA largely mirror the sensitive data standards of the *EU Privacy Directive*, as outlined in Section III.C.1, above, there are some differences. For example, the *EU Privacy Directive* offers some standards to clarify the meaning of consent. As noted, however, the DPA provides no specific standard or definition of terms such as "explicit consent." Nor does the DPA specify the scope and meaning of the term "medical research," which is distinguishable from "health research." Whether the term "medical research" includes epidemiological public health research would seem important, since medical research constitutes one exception to the general requirement of explicit consent for processing sensitive personal data. In contrast to the DPA, "medical research" in the *EU Privacy Directive* is not explicitly listed along with medical diagnosis and the like initiatives under the "medical purposes" exception to the general requirement of explicit consent to the processing of health data. Its inclusion in the DPA thus seems to accord with the general "substantial public interest" exception under Article 8 of the *EU Privacy Directive*. As the analysis in Section III.C.1, above indicates, that exception enables member states to designate the

---

69 United Kingdom, Secretary of State. *The Data Protection (Processing of Sensitive Personal Data) Order 2000: Statutory Instrument 2000 No. 417.* London, February 2000, para. 9.

70 Strobl J, Cave E, Walley T. Data Protection Legislation: Interpretation and Barriers to Research, *BMJ*, 2000;321:890-892. Warlow C. Using Patient-Identifiable Data for Observational Research and Audit, *BMJ*, 2000;321:1031-1032

processing of other categories of sensitive data as "necessary" to advancing a "substantial public interest." As per the provisions of the *EU Privacy Directive*, then, the UK Parliament appears to have deemed medical research a necessary and "substantial public interest."

d. Consent: Data Collection, Use and Disclosure

The data collection standards of the DPA reflect, among other things, the original data-quality control principles of the *OECD Guidelines*, the requirements under the *EU Privacy Directive*, and various standards from other international norms. For instance, the *OECD Guidelines* are reflected as modified in the eight central principles that guide data protection practices of the DPA. Under the *Data Protection Principles* outlined in Schedule 1 of the DPA, personal data collected in the UK generally must be: (1) fairly and lawfully processed; (2) processed only for specified purposes and not in any manner incompatible with those purposes; (3) adequate, relevant and not excessive; (4) accurate; (5) retained no longer than necessary for its purposes; (6) processed in accordance with the data subject's rights; (7) secure; and (8) not transferred to countries without adequate protection.

On the basis of these guiding principles, particular sections of the DPA refine and elaborate or qualify the principles into standards. For example, various sections of the DPA outline a data subject's general rights. Schedules 2 and 3 indicate that processing must generally be done with the consent of the data subject, unless particular exceptions apply. (The exceptions are outlined below.) While the *EU Privacy Directive* defines a valid consent as being voluntary, specific and informed, this standard does not explicitly appear in the DPA. The Act is also silent on the question of substitute decision making.

e. Exceptions and Research

Sections 28 to 38 of the DPA outline exemptions from the general data processing requirements, as well as some particular ones relevant for research. All of the exemptions reflect a societal effort to balance privacy protection with other pressing societal needs and values.

Generally consistent with the *EU Privacy Directive*, the DPA provides some general exemptions. Exceptions are, for example, defined for purposes of criminal and legal proceedings, if required by other laws, or those judged by the Secretary of State as "necessary for safeguarding" the interests of the data subject or the rights and freedoms of other individuals.

The DPA also provides specific exceptions directly relevant to research. The necessity exceptions for conducting non-consensual data processing of identifiable health information are outlined above. As indicated, "medical research" figures expressly as one of those "necessary exceptions." Moreover, under Section 33, "personal data processed only for research purposes" are exempted from some data collection principles. The application to "personal data" raises the issue of whether personal health data processed "only for research purposes" are likewise exempted, or whether they need comply with the sensitive data protection standards of the DPA, such as the requirement that such processing be done only if shown to be necessary for medical research and undertaken by one who has an obligation of professional secrecy equivalent to that of a health professional. Section 33 offers some definition of "research purposes" by stating that "research purposes includes statistical or historical purposes." Processed data that meet these initial

qualifications may be stored indefinitely and may be further processed again only for research purposes. Furthermore, such data are not subject to the general right of access provisions of the Act if the data are further processed under a range of particular conditions, which include that processing is unlikely to cause substantial harm to a data subject and that the results of the research are made available in a non-identifying form. Again, these reflect the standards of the *EU Privacy Directive*. As noted above, *Government Statutory Instrument 2000 No. 417*, on sensitive personal data, outlines standards for processing data "necessary for research purposes" that are in "the substantial public interest."

f. Data Retention and Security

As a general rule, the DPA adopts the security and data retention standards of the original *OECD Guidelines*. Under the general DPA Principle 5, personal data should be retained no longer than is necessary to accomplish the specific purposes for which it was collected. However, under Section 33, data processed "only for research purposes" may sometimes be retained for an indefinite length of time if done so in compliance with relevant conditions. These include that data are processed in a way that substantial damage or distress is unlikely to be caused to any data subject. Principle 7 also imposes a general duty to undertake "appropriate technical and organizational measures" against unauthorized, unlawful processing and accidental loss and destruction of data. It adopts the *EU Privacy Directive* balancing standard for measuring what is "appropriate": acknowledging cost and technological factors, the level of security should be appropriate to the nature of the data and the harms that may result from wrongful or remiss processing of data. Under this test, the protections for sensitive data should be higher.

g. Other Noteworthy Provisions

Several provisions of the DPA are intended to advance its implementation consistent with the *EU Privacy Directive* and Britain's public policy needs.

Under the Act, for instance, the Data Protection Commissioner is appointed to administer, with independent oversight, the provisions of the DPA. This provision responds to the requirement for an independent supervisory authority to oversee data protection principles under the *EU Privacy Directive*. Sections 51 to 54 of the DPA indicate that the Commissioner is to discharge such duties by both education and enforcement roles.

Other sections are designed to further effective implementation. For example, Section 67(2) of the Act empowers the UK Secretary of State to issue orders and regulations that advance the principles and provisions of the DPA. The process must include initial consultation with the Data Protection Commissioner. Accordingly, the Secretary of State has acted under these provisions to issue statutory instruments that address, among other things, international data sharing, a code of practice for media organizations, and sensitive personal information. Some of these instruments have been noted above.

2. *Confidentiality Guidelines of the British Medical Association (BMA)*

In 1999, as part of a public policy response to the UK DPA, and to assist its membership, the British Medical Association released Guidelines on the *Confidentiality and Disclosure of*

Health Information.[71] The Guidelines address a variety of facets of the ethics of confidentiality, including research. They contribute to an ongoing process pursued by the BMA for years to seek public policy and statutory clarification of the medical law of confidentiality. The Guidelines indicate that while the DPA made advances in this respect, the BMA still supports further legislative initiatives.

In this context, the Guidelines, considering identifiable health information to be a special and sensitive category of data, define several concepts directly relevant to health research:

- **Confidentiality**: The principle of keeping secure, and secret from others, information given by or about an individual in the course of a professional relationship.
- **Disclosure**: The revealing of identifiable health information to anyone other than the subject.
- **Personal health information**: Any personal information relating to the physical or mental health of any person from which that person can be identified.
- **Anonymized information**: Information which does not, directly or indirectly, identify the person to whom it relates.

On the basis of such concepts, the Guidelines outline elements for discharging the general duty of confidentiality and reasonable limits thereon. They underline the societal need for the traditional duty of medical secrecy, for example, by identifying a "strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it." In terms of limits, the Guidelines maintain that research constitutes a justifiable use of personal health information under particular conditions. To balance respect for confidentiality and such societal needs, the Guidelines suggest that the information disclosed should be "the minimum necessary to achieve the objective." This echoes a theme sounded in the *OECD Guidelines*, as noted in Section III. A, above. To minimize infringements of confidentiality, the BMA Guidelines further indicate that research should use anonymized data whenever possible. For information that cannot be anonymized, the BMA Guidelines urge the use of pseudonyms or other tracking mechanisms to help to ensure accuracy and minimize the use of personal identifiers.

The BMA Guidelines also address consent and information. The Guidelines encourage health research organizations and professionals to educate and to share information on research, since patients may not be aware of how anonymized data can help health research that benefits society. The Guidelines outline a general requirement that consent to the disclosure of personal information be voluntary, specific and informed. The Guidelines then review a range of potential exceptions for non-consensual disclosures, such as disclosure for litigation purposes, adverse drug reaction or professional regulatory matters. In the view of the BMA, truly non-identifying data raise fewer confidentiality and consent issues. Hence, the Guidelines maintain that it is not ethically necessary to seek consent for the use of anonymous information.

[71] British Medical Association. *Confidentiality and Disclosure of Health Information*. London, October 1999. Online: www.bma.org.uk (ethics/guidelines)

3. *Medical Research Council Guidelines on Research and Personal Data*

A year after the British Medical Association released its document, the Medical Research Council (MRC) of Britain published new ethical guidelines on the use of personal information in medical research.[72] These update previous guidelines on medical research that the MRC has been periodically releasing since the 1970s.

a. Scope

In contrast to the BMA Guidelines, those of the British MRC exclusively address the research domain and are intended to guide researchers funded by the MRC. The *Medical Research Council Guidelines on Research and Personal Data (MRC Guidelines)* address all personal information and therefore have broader scope than does the DPA, as noted in the definition section below.

b. Definitions

The *MRC Guidelines* outline a glossary of definitions directly pertinent to modern health research. These include definitions of "personal information, " "anonymized data"[73] (both linked and unlinked), "coded data,"[74] "confidential information"[75] and "sensitive information."[76] The definition of "personal information" is broader than the definition of personal data under the DPA. It encompasses "all information about individuals living or dead," including "written and electronic records, opinions, images, recordings and information." The guidelines also refer to and rely on "personal data," as defined in the DPA, which concerns personal information from which one may be identified either (a) from the data or (b) from combinations of the data and other information that the person in control of the data has or is likely to have in the future.

c. Special Protections: Sensitive Data

The glossary of the guidelines defines "sensitive information": "the terms "sensitive" is used in this guide to highlight the need for extra care in using information about mental health, sexuality and other areas where revealing confidential information is especially likely to cause embarrassment or discrimination." The definition parallels the concepts defined in the *COE Convention 108/1981*, as modified and incorporated into the *EU Privacy Directive*. (See Section III, above.)

---

72 Medical Research Council (Britain). *Personal Information in Medical Research (Ethics Series)*. London, 2000. Online: http://www.mrc.ac.uk/PDFs/PIMR.pdf

73 Anonymized data: "are data prepared from personal information, but from which the person cannot be identified by the recipient of the information. The term is used in the guide when referring to linked and unlinked anonymized data together."

74 Coded data: "is identifiable personal information in which the details that could identify people are concealed in a code, but which can be readily decoded by those using it. It is not anonymized data."

75 Confidential information: "is any information obtained by a person on the understanding that they will not disclose it to others, or obtained in circumstances where it is expected that they will not disclose it. The law assumes that whenever people give personal information to health professionals caring for them, it is confidential as long as it remains personally identifiable."

76 Sensitive information: "is used to highlight the need for extra in using information about mental health, sexuality and other areas where revealing confidential information is especially likely to cause embarrassment or discrimination."

d. Consent: Data Collection, Use and Disclosure Standards

Section 2 of the *MRC Guidelines* outlines a set of general principles that impose responsibilities and duties on researchers and institutions regarding the collection, use and disclosure of personal health information. These duties include:

- maintaining the confidentiality of personal information obtained in health research care
- informing people about the use of such information
- ensuring that "explicit consent" is secured for the collection, retention, and use of personal information
- designing research that observes confidentiality and consent principles
- seeking independent ethics review of research using identifiable personal information or anonymized data
- anonymizing or coding personal information as much as possible
- ensuring that personal information is handled only by those with a duty of confidentiality equivalent to that of health professionals.

e. Exceptions and Research

While the *MRC Guidelines* indicate that most health research may be conducted by respecting confidentiality and securing explicit consent for the processing of personal health information, the guidelines outline standards for the non-consensual but justified use of such information.

Article 2.2 indicates that the circumstances arise under narrow and exceptional condition: that is, "when consent is impracticable, confidential information can 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." When such circumstances are met, the "infringement of confidentiality must be kept to a minimum." These criteria impose conditions equivalent to the "necessity" and balancing standards of the *EU Privacy Directive*, the ECHR and the *OECD Guidelines*.

Article 5.1 details considerations in the coding and anonymization of processing health information, which may sometimes make these processes a practical and effective alternative to non-consensual processing. Article 3.6.6 indicates that "impracticability" may be caused by the sheer size of a research population group for some epidemiological studies, or, in more rare instances, by the risk that individual consent may in fact cause harm, as in some mental health studies. Article 4 of the guidelines outlines some examples of the non-consensual use of personal health information. Article 3.1 of the guidelines generally suggests, however, that precise judgements on the non-consensual processing of personal health information should be made on a case-by-case basis in accordance with general ethical and legal principles, again taking into account such factors as necessity, sensitivity, importance, safeguards, independent review, and expectations.

f. Data Retention and Security

Article 7 of the *MRC Guidelines* outlines the rationales and standards for storage and retention: research records need to be preserved for a long term for such reasons as the scientific validation

of research, for future research or audits, and sometimes for clinical treatment purposes. Article 7.12 suggests that for clinical and public health research and for adverse effects documentation, research should be retained some 20 to 30 years. Both research teams and universities have important responsibilities for such long-term retention, including that proper custodians are designated, records are archived in secure repositories, and the information is treated in confidence. Article 2.1 includes within its general principles the duty of principal investigators to take "personal responsibility for ensuring … that training, procedures, supervision and data security arrangements are sufficient to prevent unauthorized breaches of confidentiality." Article 5.3 elaborates this general principle into a checklist of responsibilities for data processing in an electronic or physical environment. The responsibilities include written procedures addressing such elements as the research team, regular review and revisions, software management, and disaster recovery arrangements.

(There is no description of the category "Other Noteworthy Provisions" for the Medical Research Council Guidelines on Research and Personal Data).

F. United States

Federal laws and initiatives governing the protection of personal information in the United States (US) differ from, as well as parallel, those of other nations surveyed in this report. Like all the countries examined, the US has signed and ratified the CCPR. It thus has international privacy obligations. For over a quarter of a century, federal law has imposed legal standards on the federal government's processing of personal information. The American law is one of the oldest among those in the countries surveyed.

Yet in contrast to many of those countries, the US has no central or omnibus data protection law. Instead, it tends to rely on the development of detailed federal privacy standards for different sectors of society. Consistent with this sectoral approach, the US government has recently finalized national norms for the protection of personal health information. It has also recently concluded an initiative, called the Safe Harbor Framework, that outlines national privacy standards that will harmonize American standards with those of the European Union. The following text outlines the *Federal Privacy Act*, then highlights the new federal regulation on health information privacy and the Safe Harbor Framework.

1. *Federal Privacy Act (1974)*

The *Federal Privacy Act* of 1974[77] governs federal agencies' collection, use and dissemination of personal information. The Act applies to personal information generally, including health information held by federal agencies such as the Indian Health Service and like entities of the federal department of health. Like the *OECD Guidelines* that would follow, the Act is premised on the idea that individuals have a right to know what personal information the government holds about them and how that information will be used, as well as having the right to review the information. It requires agencies to apply basic fair-information practices, including safeguards

[77] 5 *United States Code*, Sec. 552a, as amended. Online: www.usdoj.gov/04foia/04_7_1.html

for the security and confidentiality of records. The practices are based on the *Code of Fair Information Practice Principles*[78] that the US Department of Health established in 1973.

The Act requires federal agencies to specify the purposes for collecting personal information and provides civil and criminal penalties for its misuse. Unless a proposed disclosure falls within enumerated exceptions, the Act prohibits disclosure of that information without the prior written consent of the data subject. The exceptions include (a) information collected solely as statistical research if transferred in a non-identifiable manner, (b) compelling circumstances affecting the health and safety of an individual, and (c) administratively determined disclosures by the agency. Disclosures under the latter must still be "compatible" with the purpose for which the information was collected.

Some aspects of the implementation of the *Federal Privacy Act* differ from those found in other countries. In contrast to privacy commissioners and like independent overseeing bodies found in other countries, for example, the Office of Management and Budget plays a limited role in setting policy for federal agencies.[79] In 1999, the Office of the Chief Counselor for Privacy was created within the Office of Management and Budget to coordinate federal privacy policy in an advisory capacity.

2. *Federal Privacy of Personal Health Information Rule (2000)*

Finalized in December 2000 to take effect in April 2003, the federal *Standards for Privacy of Individually Identifiable Health Information* (*HIPAA Privacy Rule*) [80] are intended as national norms to protect the privacy of health data in the US. They result from the US federal government's increased interest in recent years in addressing privacy rights and administrative transactions in health care.

In 1996, the US Congress enacted federal legislation that aimed at, among other things, facilitating Americans' retention of private health insurance and easing administrative aspects of some health care transactions. The law is entitled the *Health Insurance Portability and Accountability Act of 1996* (HIPAA).[81] Sections 262 and 264 of HIPAA prove particularly relevant to the protection of privacy and administrative efficiency of health care transactions. The sections are noted in an explanation of the recently finalized privacy standards.

Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification provisions are found at section 262 of HIPAA. In section 262, Congress primarily sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus,

---

78 US Department of Health and Human Services (DHHS) *Code of Fair Information Practice Principles*, 1973.

79 Banisar D. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. Electronic Privacy Information Center (EPIC): Washington, 2000:230.

80 US Department of Health and Human Services. *Standards for Privacy of Individually Identifiable Health Information—Final Rule* (hereinafter HIPAA Privacy Rule) *Federal Register* 28 December 2000;65(250):82462, to be codified at 45 *Code of Federal Register* 160 and 164. Online: www.hhs.gov/ocr/hipaa

81 *Health Insurance Portability and Accountability Act of 1996* (HIPAA) Public Law 104-191, as amended, 42 United States Code 1320-d.

section 262 directs HHS [US Department of Health and Human Services] to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions. At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of health information.[82]

In response, proposed health information privacy standards from the US Department of Health and Human Services (HHS) were submitted to the US Congress in 1997. Section 262 of HIPAA further provided that if Congress did not enact corresponding health information privacy legislation by August 1999, then HHS would be obliged to enact final regulations by February 2001. The US Congress failed to do so, even though several bills and associated reports[83] addressed the issue. In December 2000, HHS finalized the *HIPAA Privacy Rule*.[84]

a. Scope

The *HIPAA Privacy Rule* addresses medical records and other individually identifiable health information used or disclosed by a "covered entity" in any form, which includes electronically, in writing or orally. It generally applies to "health plans," "health care clearinghouses," and those "health care providers," in either the public or private sector, who conduct certain financial and administrative transactions electronically (for example, electronic billing and funds transfers). Many US research interests will be covered under the *HIPAA Privacy Rule* as health service providers. Sections 160.201 to 160.205 of the *HIPAA Privacy Rule* indicate that it is intended to provide minimum national standards across the US. Accordingly, it generally preempts state laws that provide lower standards; it complements those that impose more stringent privacy protections.

Beyond its interaction with state laws, the scope, application and complexity of the HIPAA is augmented by its intersection and interaction with other US federal laws. For instance, the *HIPAA Privacy Rule* interacts with the *Federal Food, Drugs and Cosmetics Act*,[85] US federal policy and regulations on research involving humans,[86] and the *Clinical Laboratory Improvements Amendments* of 1988.[87] Some of these laws outline standards relevant to health research. Thus, some of the intersections between the *HIPAA Privacy Rule* and such laws are noted, but a thorough exploration of those interactions is beyond the scope of this analysis.

---

82 *HIPAA Privacy Rule*, op. cit., Part I.

83 See, e.g., United States General Accounting Office. *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited*. Washington, February 1999.

84 *HIPAA Privacy Rule*, op. cit. *Federal Register* 28 December 2000;65(250):82462, to be codified at 45 *Code of Federal Register* 160 and 164.

85 21 *United States Code Annotated* 301 et seq., as implemented in part under 21 *Code of Federal Register* 310 et seq.

86 See, e.g., US Department of Health and Human Services. (*Basic DHHS Policy for Protection of Human Research Subjects*) *Regulations on Protection of Human Subjects*. *Federal Register* 18 June 1991;56:28003, codified at 45 *Code of Federal Register* 46. Online: http://ohsr.od.nih.gov/mpa/45cfr46.php3

87 42 *United States Code* 263a, as implemented in part under 42 *Code of Federal Register* 493.3(a)(2).

b. Definitions

The *HIPAA Privacy Rule* specifies an extensive list of definitions, including those for several key terms. These include "identifiable health information," "use" and "disclosure," "health provider," "de-identified" health information, "consent," "data aggregation," and "research."

For instance, the *HIPAA Privacy Rule* regards identifying data as a subset of general health information. Section 164.501 thus provides a broad definition of "individually identifiable health information." It refers to the "past, present, or future physical or mental health or condition of an individual" that either identifies the individual or affords a reasonable basis to believe that the information can be used to identify the individual. Identifiable health information that has been de-identified may not be subject to the *HIPAA Privacy Rule* if certain provisions are respected. (See Section e., below.)

The *HIPAA Privacy Rule* does not use the term "data processing" Instead, it outlines broad definitions of the terms "use" and "disclosure." Thus, identifying health information that is shared, examined, analyzed or employed within an entity is "used," while that which is shared or transferred outside the entity is "disclosed." Definitions of other important terms are elaborated below.

c. Special Protections: Sensitive Data

The *HIPAA Privacy Rule* declares that "(a)mong different sorts of personal information, health information is among the most sensitive." The *HIPAA Privacy Rule*'s approach thus accords with that in many countries and with standards in the international community.

Within its general treatment of health information as sensitive data, the *HIPAA Privacy Rule* offers even higher protections or standards for psychotherapy notes. Psychotherapy notes are defined in Section 164.501 as notes "recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record."

The definition excludes "medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." Under Section 168.508(a)(2), the disclosure or use of such notes requires a valid authorization, except in limited circumstances. These include treatment by the originator of the notes, particular legal proceedings, or particular institutional training programs. Under Section 164.524, individuals do not have a general right of access to psychotherapy notes.

d. Consent: Data Collection, Use and Disclosure

The *HIPAA Privacy Rule* outlines general standards on the processing of health data in a manner that parallels those of the *OECD Guidelines* and *EU Privacy Directive*. Three of the standards illustrate how.

First and parallel to the *EU Privacy Directive* the *HIPAA Privacy Rule* imposes a general prohibition on the "use" and "disclosure" of "individually identifiable health information," unless consent or authorization is secured. "Consent" and "authorization" under the *HIPAA Privacy Rule* are not synonymous. Consent in writing is generally required for the use and disclosure of personal information for "treatment," "payment" and "health care purposes." The *HIPAA Privacy Rule* defines these terms. Written "authorization" is required for other purposes, which would generally include research. The *HIPAA Privacy Rule* outlines various elements that should generally be included in a valid authorization. Sections 164.508(b) and (c) provide, among other things, that a valid authorization should be written in plain language and should disclose information about: what information is to be used or disclosed; who is authorized to request the information; and who shall receive the information, and how and when they will receive it. Included should be an outline of the right to revoke the authorization. Authorizations may generally be revoked in writing at any time, unless the entity "has taken action in reliance on" the authorization. Additional requirements apply, depending on whether the authorization for use or disclosure is sought for the entity or for disclosures by others. For research that involves treatment as, for example, in some clinical trials of drugs the *HIPAA Privacy Rule* generally specifies an authorization contoured to the research treatment context. Section 164.508(f) requires the provision of, among other things, a description on how the use or disclosure of information will be used for treatment. It also requires conformity with the core consent standards of the *HIPAA Privacy Rule*, subject to applicable exceptions.

Second, the *HIPAA Privacy Rule* imposes a general duty to strictly limit the scope of any necessary invasions of personal privacy. As Section III, above, indicates, both the *OECD Guidelines* and *EU Privacy Directive* generally contemplate that any necessary invasions of privacy be limited. The *HIPAA Privacy Rule* does so by defining a general standard. Section 164.502 requires entities to make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Under Section 164.514(d), implementation of the "minimum necessary" standard requires specific organizational and administrative steps. For example, entities that disclose protected health information on a routine and recurring basis must implement policies and procedures to limit the information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. Institutions must also identify and take reasonable efforts to limit, to the minimum necessary, those personnel who have access to protected health information.

Third, the *HIPAA Privacy Rule* outlines a data subject's rights to have general and specific information about the data collected. Section 164.524, for instance, outlines the general right to inspect and to obtain a copy of one's health information, exclusive of psychotherapy notes. Section 164.522(a) outlines the right to request restrictions on uses and disclosures. Section 164.528 outlines the right to request an "accounting" of all disclosures made within the last six years.

e. Exceptions and Research

The *HIPAA Privacy Rule* outlines several exceptions to the general requirement of consent or authorization, as well as some provisions and exceptions particularly relevant for research. As in other countries, the exceptions reflect an effort to balance privacy protection with other pressing societal needs and values.

In terms of general exceptions, Section 164.512 authorizes the non-consensual use or disclosure of health information for, among other things, (a) health oversight activities, such as audits, administrative investigations, inspections, or licensor or disciplinary actions; (b) public health needs, such as for the legally authorized collection or receipt of health information for epidemiological, vital statistics or national drug and therapeutics law purposes; and (c) when necessary to prevent a serious and imminent threat to health or safety. Such provisions parallel exceptions of the *EU Privacy Directive*, as noted in Section III.C.3., above.

The *HIPAA Privacy Rule* also provides specific provisions and exceptions directly relevant to research activities. Section 164.501 of the *HIPAA Privacy Rule* defines "research" as involving "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." The *HIPAA Privacy Rule* explicitly excludes research from other important terms. Thus, even in the broad definition of "health care activities," research is explicitly excluded. The *HIPAA Privacy Rule* outlines standards relative to such research as clinical trials. Section 164.524(a)(2)(iii), for instance, provides that access to personal information may be restricted for patients in research involving treatment. Access may be suspended for the course of the research if the suspension was included in the patient's consent to the research and if the health care provider has informed the participant that access will be reinstated at the conclusion of the research. As well, the *HIPAA Privacy Rule* outlines standards to govern some non-consensual research. Standards governing the use of "de-identified information" and research that may be conducted under a waiver of the normal requirement of individual authorization or consent are two important examples. Each is outlined below.

De-identified and Coded Data: Section 164.502(d)(2) of the *HIPAA Privacy Rule* provides that health information that meets the requirements for de-identified health information will not be bound by the general use and disclosure standards of the *HIPAA Privacy Rule*. The Section refers to "de-identified" information as that which "does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify."

This complements Section 164.514(a), which outlines how the de-identification standards may be practically implemented. Under it, institutions are authorized to de-identify health information by two methods.

One approach is for a professional determination to be made that the risk of identification by the anticipated recipient, through the use of information or in combination with other reasonably available information, is "very small." This judgement can be made only by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable." The professional must apply such principles and methods to evaluate the risk. The methods and results of the analysis must be documented.

Alternatively, the entity may remove identifiers. These include names, addresses, zip codes, identifying photographic images, and voice prints; numbers for telephone, fax, medical records, licences, accounts or licence plates; or any "other unique identifying number, characteristic, or code." Such de-identification must be done without actual knowledge that the information could

be used alone or in combination with other information to identify an individual who is a subject of the information. It should be noted that under Section 164.514(c), codes to re-identify de-identified health information are authorized if appropriate security measures are observed, if the codes are not derived from or related to information about the individual, and if they are not capable of being translated to identify the individual.

Waiver of Authorization*:* Beyond the application of the general exceptions or the de-identification processes, research involving personal health information is permitted when a waiver of authorization is independently approved by a privacy board or research ethics committee. Section 164.512(i) generally outlines three conditions that must prevail for a valid waiver. These conditions contain important standards.

First, the entity seeking a waiver must secure from the researcher specific assurances or representations to prepare the research for review by the committee. Among affirmations regarding confidentiality and related requirements, the researcher must represent that the information sought is "necessary for research purposes."

Second, the waiver must be approved by a duly constituted institutional research ethics committee or by a privacy board. The privacy board must be free from conflicts of interest and must be composed of individuals from diverse backgrounds and who have "appropriate professional competency." If the waiver is authorized by a research ethics committee, the committee must meet the composition and independency standards required under US federal research law.[88] The review must also be conducted in accordance with the normal review procedures of federal research ethics law.

Third, beyond the procedural requirements, the privacy board or institutional research ethics committee must generally base the waiver on a determination that the research involves only a minimal invasion of privacy, which is justified by the importance of the research and the impracticability of otherwise undertaking it. The committee thus specifically needs to determine, among other things, that: (a) the use of personal health information involves minimal risk, (b) the waiver will not adversely affect the rights or welfare of the individuals, (c) the research could not practicably be undertaken without the waiver and without the information ("practicably" is not defined), (d) there is a reasonable relation between the privacy risks and benefits and the importance of the knowledge that may be reasonably expected to result, (e) particular data security measures are in place to protect against improper use or disclosure, and (f) the research provides adequate plans for data retention. Under the latter, such plans should provide for the destruction of identifiers "at the earliest opportunity" consistent with conduct of research, unless continued retention is authorized by law or legitimized by health or research justifications.

[88] See, e.g., 45 *Code of Federal Register* 46.107 (DHHS); 21 *Code of Federal Register* 56.107 (US Food and Drug Administration).

f. Data Security and Retention

In general, the *HIPAA Privacy Rule* imposes security standards similar to those in the original *OECD Guidelines*. Under the administrative requirement of Section 164.530, institutions "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The section also imposes a duty of "reasonably safeguarding" such information. Other provisions of the *HIPAA Privacy Rule* complement and elaborate these general standards. For instance, the administrative security measures associated with access to coded information and re-identification standards have been noted in Section e., above. As well, the "minimum necessary" standard discussed above involves the implementation of organizational and administrative safeguards for limiting access to health data. Moreover, Section 164.530 imposes a workforce training requirement to ensure that employees adhere to institutional privacy policies and procedures.

The *HIPAA Privacy Rule* seems not to have a separate, explicit and detailed standard for length of data retention. Instead, it appears to address the issue indirectly through other standards. For example, reference is made to data retention in the standards relied on by research ethics committees to evaluate whether a waiver should be granted for the normal requirement of individual authorization for health research. As indicated, research protocols should include plans for the destruction of identifiers "at the earliest opportunity" consistent with conduct of research, unless continued retention is authorized by law or legitimized by health or research justifications. Though the precise language and focus on research differ, the intent seems to parallel the reasonable retention standards of the original *OECD Guidelines*.

g. Other Noteworthy Provisions

Several provisions of the *HIPAA Privacy Rule* are intended to advance its implementation nationally and institutionally. Some of the provisions parallel and some depart from analogous provisions for implementing new data protection or privacy laws in other countries surveyed in this report. Oversight and enforcement of the *HIPAA Privacy Rule*, for instance, are delegated to the Office for Civil Rights (OCR) in the HHS. The OCR will assist providers, plans and health clearinghouses in meeting the requirements of the *HIPAA Privacy Rule*. The OCR also is responsible for receiving and investigating privacy complaints. In other countries, nearly exclusive and independent oversight and implementation is typically entrusted to a separate government entity, such as a data protection or privacy commission.

Institutionally, the *HIPAA Privacy Rule* imposes standards for implementation. For instance, Section 164.530's administrative standards require covered entities to adopt written privacy procedures concerning access, use and disclosure of protected information. They are also required to train employees and designate a privacy officer, who is to ensure that privacy procedures are followed.

Section 164.520 also imposes on covered entities a general duty to provide individuals with a written notice, in plain language, of privacy practices for protected health information. The notice must include, among other things, information about use and disclosure, individual rights, institutional privacy duties, and contact persons. The notice must be timely, accurate and regularly revised. Specific notice standards are further required for health care providers in direct-treatment relationships.

Finally, in contrast with the *OECD Guidelines* and the *EU Privacy Directive*, the *HIPAA Privacy Rule* outlines no explicit provisions regarding the sharing of health information with other nations. Instead, those provisions have come from a broader, separate initiative.

3. *Safe Harbor Privacy Principles (2000)*

Like many countries, the US has recently undertaken initiatives aimed at harmonizing national privacy standards with the provisions of the *EU Privacy Directive*. As noted in Section III.C, above, Article 25 of the Directive generally prohibits the transfer of personal data from EU member nations to those lacking an "adequate level of protection." In the absence of a uniform or central data protection statute in the US, the US Department of Commerce has sought to institute standards that would enable US companies to be included in the transfer of personal information from Europe. Following some two years of deliberations, negotiation and revision after an initial US proposal of 1999, the US and EU approved the final *US Safe Harbor Privacy Framework*[89] in July 2000. The Framework consists of a number of documents from the US and the EU. The key documents include the US Department of Commerce's *Safe Harbor Privacy Principles* and the *Frequently Asked Questions* (FAQs).

a. Scope

The Principles "are intended for use solely by US organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of 'adequacy' it creates." The Principles apply to electronic or manual information processed by US companies that voluntarily agree to adhere to the Safe Harbor Principles so the companies may obtain and retain the benefits of participation. They apply for as long as the organization stores the relevant personal information, even if the organization has otherwise concluded its participation in a safe-harbor program.

b. Definitions

The Principles define personal information broadly. "Personal information" or "personal data" refers to "data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the European Union, and recorded in any form." Hence, the Principles adopt the standard of personal data of the *EU Privacy Directive*.

c. Sensitive Data

The *Safe Harbour Principles* offer heightened protections for sensitive data. This includes personal information specifying racial or ethnic origins, sexual preferences, or medical or health conditions. The Choice Principle generally prohibits the use of sensitive information unless the data subject has specifically agreed to its use. The approach accords with most modern international standards.

---

89 US Department of Commerce. *Safe Harbor Framework*. Washington, July 2000. Online: www.export.gov/safeharbor/sh_documents.html

d. Consent: Data Collection, Use and Disclosure

At the core of the *Safe Harbor Framework* lies a set of seven privacy principles that parallel those outlined in the original *OECD Guidelines*, as modified by the *EU Privacy Directive*. The *Safe Harbor Privacy Principles* are the following:

- Notice
- Choice
- Onward Transfer (for example, third-party use)
- Security
- Data Integrity
- Access
- Enforcement.

The Principles outline the general standards for the processing of personal data under the *Safe Harbor Framework*. A complementary listing of FAQs on 15 issues outlines explanations, refinements, context and some exceptions to the Principles.

Thus, for instance, the Notice and Choice principles generally define collection and use standards grounded on informed consent.

The Notice Principle requires that institutions give data subjects information "about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure."

The provision of such information complements the consent standards of the Choice Principle. As the FAQ on "Choice" explains, "the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices." Thus, individuals have the option to choose whether their personal information may be disclosed to a third party or used for "a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual." To make such choices, the information must be provided when the data subject is first approached about the use of personal information, or as soon as "practicable" thereafter. The Onward Transfer Principle generally provides that the notice and choice standards apply to sharing information with third parties. The Data Integrity Principle outlines a standard relevant to secondary uses on the basis of an "incompatible purpose" standard. It provides that an organization "may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."

e. Exceptions and Research

The *Safe Harbour Framework* outlines both general exceptions and provisions and exceptions directly relevant to research. The Framework generally indicates that adherence to the Principles may be limited: "(a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited

to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts." "Public interest" is not defined, and differs somewhat from the "substantial public interest" language of the *EU Privacy Directive*. Still, as with the *EU Privacy Directive*, *HIPAA Privacy Rule*, and *OECD Guidelines*, the Framework outlines a necessity standard to justify invasions of privacy. Under the standard, necessary invasions of privacy also generally have to be limited to the degree necessary to achieve their purpose(s).

The Framework also outlines provisions and exceptions for research. FAQ 1, for instance, outlines exceptions to the general prohibition against use of sensitive data such as personal health information. These include when, among other situations, the processing is in the vital interests of the data subject, required to provide medical care or diagnosis, or necessary for particular legal proceedings. These mirror exceptions under the *EU Privacy Directive*.

FAQ 14 directly addresses questions of the use of identifiable health information in pharmaceutical and medical-products research. It offers interpretations or clarifications on such matters as anonymity, coding, secondary use, and the application of EU versus US standards on information received in the US from Europe. It indicates that particularly coded data received from an EU country may not be bound by the principles under particular circumstances. The FAQ indicates that this would be so when, for instance, a European principle investigator uniquely codes the data so as to make it non-identifying to a sponsoring pharmaceutical company and US researchers. FAQ 14 also outlines a related general rule: research data used for pharmaceutical research and other purposes should be anonymized when appropriate. It further indicates that secondary use of data transferred from Europe is authorized when it is consistent with the general research purposes of the original collection or when a new consent has been obtained. To avoid ambiguity over consistent or inconsistent purposes, FAQ 14 suggests that informed consent for research might include an explanation that future needs for unspecified or unanticipated research on an individual's personal data might arise, given the nature of research.

f. Data Security and Retention

The Security Principle obliges adherents to Safe Harbor standards to take "reasonable precautions" to protect personal data from unauthorized access, misuse, destruction, alteration or loss. The Framework seems not to outline an explicit standard on the length of data retention.

g. Other Noteworthy Provisions

General oversight and enforcement of the Framework has been assigned to the Federal Trade Commission (FTC), an independent regulatory body associated with the US Department of Commerce. Such enforcement includes the review of and response to privacy complaints. Entities that undergo the formal written process of self-certifying to the Department of Commerce of their adherence to the Principles must accept the enforcement authority of the FTC. The limited scope of the FTC has caused concern to EU analysts.

Bibliography

This bibliography is presented in three parts:

- **General Works**
- **International Organizations**
- **Countries**

General Works

Annas G.J., Grodin M.A. *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation.* Oxford University Press: New York, 1992: 94-104.

Banisar D. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. Electronic Privacy Information Center (EPIC): Washington, 2000.

Callens S. The Privacy Directive and the Use of Medical Data for Research Purposes. *European J. Health L.* 1995;2:309-340.

Mason J.K, McCall Smith R.A. *Law and Medical Ethics.* 4th ed. Butterworth's: London, 1994.

Michael J. *Privacy and Human Rights.* UNESCO and Dartmouth Publishing: Paris, 1994.

Treseder P., Williams P. The Common Principles of Health Informatics Standardisation that Require Exchange of Information Between the Standardisation Bodies of Different Countries. *Int. J. Med. Inf.* 1998;48:39-42.

Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10., Vol. 2. *Washington, D.C.: U.S. Government Printing Office, 1949.*

International Organizations

Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4 November 1950, E.T.S. No. 5, 213 U.N.T.S. 222. Online: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, E.T.S. No. 108. Online: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

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, E.T.S. No.164. Oviedo, 1997. Online: http://conventions.coe.int/Treaty/EN/cadreListeTraites.htm

Draft Additional Protocol to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No 108) Regarding Supervisory Authorities and Transborder Data Flows and Explanatory Report. Strasbourg, 2000. Online: http://stars.coe.fr/ta/TA00/eopi217.htm

European Court of Human Rights. *M.S. v. Sweden*, 27 August 1997, para. 41. See also *Z. v. Finland*, 25 February 1997, 45 B.M.L.R.107.

Recommendations of the Council of Europe

Recommendation No. R(83)10 on the Protection of Personal Data Used for Scientific Research and Statistics. Strasbourg, 1983.

Recommendation No. R(91)10 on the Communication to Third Parties of Personal Data Held by Public Bodies. Strasbourg, 1991.

Recommendation No. R(97)18 on the Protection of Personal Data Collected and Processed for Statistical Purposes. Strasbourg, 1997.

Recommendation No. R(97)5 of the Committee of Ministers to Member States on the Protection of Medical Data. Strasbourg, 1997. Online: http://cm.coe.int/ta/rec/1997/97r5.html

Explanatory Memorandum, Recommendation No. R97(5) of the Committee of Ministers to Member States on the Protection of Medical Data, par. 41, 43 and 44. Online: http://cm.coe.int/ta/rec/1997/ExpRec(97)5.htm

European Union

European Group on Ethics in Science and New Technologies to the European Commission. *Ethical Issues of Healthcare in the Information Society*. Opinion No. 13, 30 July 1999. Online: http://europa.eu.int/comm/european_group_ethics/docs/avis13_en.pdf

European Parliament and Council of Europe. *Charter of Fundamental Rights*. Nice, 2000. Online: http://www.europarl.eu.int/charter/default_en.htm

European Parliament and Council of Europe. *Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data*. Official Journal L 281, 23/11/1995 p. 0031-0050 Online: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0045.html

Organization for Economic Co-operation and Development (OECD)

Explanatory Memorandum, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. para. 54-55. OECD: Paris, 1981. Online: http://www1.oecd.org/dsti/sti/it/secur/prod/priv-en.htm

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD: Paris, 1981. Online: http://www.oecd.org/dsti/sti/it/secur/prod/priv_en.htm

Ministerial-Level Conference. *A Borderless World: Realising the Potential of Global Electronic Commerce.* See the Ministerial Declaration on the Protection of Privacy on Global Networks. Online: http://www.oecd.org/dsti/sti/it

United Nations

Guidelines for the Regulation of Computerized Personal Data Files. Adopted by General Assembly Resolution 45/95 of 14 December 1990. New York, 1990. Online: http://www.unhchr.ch/html/ menu3/b/71.htm

International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966. Can. T.S. 1976 No.47, 999 U.N.T.S. 171. Online: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

International Covenant on Economic, Social and Cultural Rights. Adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966.

United Nations Charter, Preamble. San Francisco: United Nations, June 1945.

Universal Declaration of Human Rights. New York: United Nations, Adopted by General Assembly Resolution 217A (III) of 10 December 1948. Online: http://www.unhchr.ch/udhr/lang/eng.htm

Unesco, *Universal Declaration on the Human Genome and Human Rights.* Paris, 1997. Online: http://www.unesco.org/ibc/en/genome/projet

Unesco, Working Group of the International Bioethics Committee on Confidentiality and Genetic Data. *Report on Confidentiality and Genetic Data.* Paris, June 2000.

World Health Organization European Consultation on the Rights of Patients. *A Declaration on the Promotion of Patients' Rights in Europe.* Amsterdam, 1994. Reprinted in *European J. Health L.* 1994;1:279-291. Online: http://www.who.int/library/reference/information/declarations/index.en.shtml

World Medical Association

Declaration of Geneva: A Physician's Oath. Geneva, 1948, as amended.

Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects. Helsinki, 1964. Online: http://www.wma.net/e/policy/17-c_e.html

Declaration of Helsinki: *Ethical Principles for Research Involving Human Subjects*. Edinburgh, 2000. Online: http://www.wma.net

Statement on the Use of Computers in Medicine, based on Resolution of the 27th World Medical Assembly in Munich, October 1973, as amended by the 35th World Medical Assembly in Venice, Italy, October 1983.

The 27th World Medical Assembly: Munich, October 14–20, 1973. *World Med. J.* 1974(2)4-10.

Countries

Australia

National Health and Medical Research Council

Guidelines Under Section 95 of the Privacy Act 1988. Canberra, 2000. Online: http://www.health.gov.au/ nhmrc/issues/researchethics.htm

National Statement on Ethical Conduct in Research Involving Humans. Canberra, 1999.

Joint National Health and Medical Research Council/Australian Vice-Chancellors' Committee Statement and Guidelines on Research Practice (1997).

Office of the Privacy Commissioner

Draft Health Privacy Guidelines. Canberra, 14 May 2001. Online: http://www.privacy.gov.au

National Principles for Fair Handling of Personal Information, Australia. Canberra, 1999. Online: http://www.privacy.gov.au/news/health.html

Parliament of the Commonwealth of Australia, House of Representative Standing Committee on Legal and Constitutional Affairs. *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*. Online: http://www.aph.gov.au/house/committee/laca/privacybill/contents.htm

Privacy Act 1988. Act No. 119 of 1988, as amended. Online: http://www.austlii.edu.au

Privacy Amendment (Private Sector) Act 2000. Act No. 155 of 2000, amending the *Privacy Act 1988.* Online: http://www.privacy.gov.au

*The Private Sector: National Privacy Principles. S*ee *Privacy Amendment (Private Sector) Act 2000*.

The Public Sector Standards: Information Privacy Principles. See *Privacy Amendment (Private Sector) Act 2000*. Senate Debate on Privacy Amendment (Private Sector) Bill. Online: http://www.law.gov.au/privacy/senatedebate.htm

The Commonwealth of Australia Constitution Act. Online: http://www.republic.org.au/const/cconst.html

Canada

Canadian Institutes of Health Research. *A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research.* Public Works and Government Services Canada: Ottawa, 2000. Online: http://www.cihr.ca

Personal Information Protection and Electronic Documents Act. S.C. 2000. c.5. Online: http://www.privcom.gc.ca

France

Braibant G. *Données personnelles et société de l'information* : *Rapport au Premier Ministre sur la transposition en droit français de la directive numéro 95/46*. Paris, 3 mars 1998. Online: http://www.cnil.fr/textes/indextranspo.htm

Code civil. Online: http://www.legifrance.gouv.fr/citoyen/new_code.ow

Code de déontologie médicale. Online: http://www.legifrance.gouv.fr/citoyen/new_code.ow

Code pénal. Online: http://www.legifrance.gouv.fr/citoyen/new_code.ow

Conseil Constitutionnel. *Décision 94-352* du 18 janvier 1995.

Décret n° 78-774, du 17 juillet 1977. *Journal Officiel* du 23 juillet 1997.

Décret n° 95-682 du 9 mai 1995. *Journal Officiel* du 11 mai 1995.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Journal Officiel du 7 janvier 1978. Online: http://www.legifrance.gouv.fr

Loi n° 79-18 du 3 janvier 1979 relative aux archives, Journal Officiel du 5 janvier 1979: 49, corrected in *Journal Officiel* du 6 janvier 1979:55. Online: http://www.cnil.fr/textes/text052.htm

Loi nº 94-548 du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la *loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. *Journal Officiel* du 2 juillet 1994.

National Data Processing and Liberties Commission (La Commission nationale de l'informatique et des libertés [CNIL]). Traitements des données de santé à caractère personnel. délibération nº 97-008 du 4 février 1997. *Journal Officiel* du 12 avril 1997. Online: http://www.cnil.fr

Netherlands

Constitution of the Kingdom of the Netherlands 1989, art. 10.

Ploem M.C. Medical Research and Informational Privacy, *Medicine and Law* 1998;17: 287-297.

Wet bescherming persoonsgegevens (*Personal Data Protection* Act). 6 July 2000. Staatsblad 2000 302 (unofficial translation). Online: http://www. registratiekamer.nl/; http://home.planet.nl/~privacy1

Wet geneeskundige behandelingsovereenkomst (*Medical Treatment Contract Act, Act of 17 November 1994, amending the Civil Code and Other Legislation in Connection with the Incorporation of Provisions Concerning the Contract to Provide Medical Treatment*). Stb 1994, 837.

Wet persoonsregistraties (*Law on Registration of Personal Data*). 28 December 1988. The Dutch Data Registration Act, 1988. Online: http://home.planet.nl/~privacy1

New Zealand

Application by L. (1997) 3 HNRX 716 (Complaints Review Tribunal)

Health Act 1956, as amended. Reprinted Statutes of New Zealand 1993; 31(1): 467-563.

Health (Retention of Health Information) Regulations 1996, adopted under section 121 of the *Health Act 1956*, as amended.

Privacy Act 1993. Online: http://www.privacy.org.nz/recept/rectop.html

Privacy Commissioner of New Zealand

Discussion Paper No. 12: New Privacy Protections. Auckland, 1998.
Online: http://www.privacy.org.nz/slegisf.html

Health Information Privacy Code 1994, as amended. Auckland, 1994; revised edition, 2000.
Online: http://www.privacy.org/nz/recept/rectop.html

Von Tigerstrom B. The Hidden Story of Bill C-54: The Personal Information Protection and Electronic Documents Act and Health Information. *Health Law Rev.* 1999*:8(2)*:12.

United Kingdom

British Medical Association. *Confidentiality and Disclosure of Health Information*. London, 1999. Online: http://www.bma.org.uk (ethics/guidelines)

Data Protection Act, 1998. c. 29, superseding the *Data Protection Act* of 1984. Online: http://www.dataprotection.gov.uk

Human Rights Act, 1998. c. 42.

Medical Research Council (Britain). *Personal Information in Medical Research (Ethics Series)*. London, 2000. Online: http://www.mrc.ac.uk/PDFs/PIMR.pdf

Strobl J., Cave E., Walley T. Data Protection Legislation: Interpretation and Barriers to Research. *BMJ* 2000; 321:890-892.

United Kingdom, Secretary of State. *The Data Protection (Processing of Sensitive Personal Data) Order 2000: Statutory Instrument 2000 No. 417*. London, February 2000; para. 9.

United Kingdom, Secretary of State. *The Data Protection (Subject Access Modification) (Health) Order 2000: Statutory Instrument 2000 No. 413*. London, February 2000.

Warlow C. Using Patient-Identifiable Data for Observational Research and Audit. *BMJ* 2000; 321:1031-1032.

United States

Clinical Laboratory Improvements Amendments, 1998. 42 United States Code 263a, as implemented in part under 42 *Code of Federal Register* 493.3(a)(2).

Federal Food, Drugs and Cosmetics Act. 21 United States Code 263a, as implemented in part under 42 *Code of Federal Register* 493.3(a)(2).

Federal Privacy Act, 1974. PL 93-579,5 USC 552a, as amended. Online: http://www.epic.org/privacy/laws/privacy_act.html

Freeman P., Robbins A. US Health Data Privacy Debate: Will There be Comprehension Before Closure? *Int. J. Technol. Assess. Health Care* 1999;15(2):316-331.

General Accounting Office. *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited.* Washington, February 1999.

Health Insurance Portability and Accountability Act of 1996. PL 104-91, as amended, 42 USC 1320-d. Online: http://aspe.hhs.gov/admnsimp/pvcrec0.htm

Heroic Assemblage of Information About State Laws by Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, Shows Complexity. The State of Health Privacy: An Uneven Terrain (1999). Online: http://www.healthprivacy.org/info-url_nocat.htm

Hodge J.G., Gostin L.O., Jacobson P.D. Legal Issues Concerning Electronic Health Information: Privacy, Quality and Liability. *J. Amer. Med. Assoc.* 1999;282;1466-1471.

Public Health Service Act, as amended, 42 USC 241(d) and 299dd-2. Regulations at 42 CFR Part 2.

United States Privacy Protection Study Commission. Personal Privacy in an Information Society: Report of the Privacy Protection Study Commission. Washington, 1977.

US Department of Commerce. *Safe Harbor Framework.* Washington, July 2000. Online: http://www. export.gov/safeharbour/sh_documents.html

US Department of Health and Human Services (DHHS)

(*Basic DHHS for the Protection of Human Research Subjects*). Regulations on Protection of Human Subjects. Federal Register 18 June 1991; 56: 28003, 45 Code of Federal Register 46. Online: http://ohsr.od.nih.gov/mpa/45cfr46.php3

US Department of Health and Human Services (DHHS) *Code of Fair Information Practice Principles,* 1973.

Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996. Washington, September 1997. Online: http://aspe.hhs.gov/admnsimp/pvcrec0.htm

Standards for Privacy of Individually Identifiable Health Information—Final Rule. Fed. Reg. 28 December 2000:65(250) 82467. Online: http://www.hhs.gov/ocr/hipaa