Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 10-Dec-1999
Dist. : 13-Dec-1999

English text only

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR SCIENTIFIC AND TECHNOLOGICAL POLICY

DSTI/STP/BIO(99)3/FINAL
Unclassified

Working Party on Biotechnology

HEALTH POLICY BRIEF

DATA PROTECTION IN TRANSBORDER FLOWS OF HEALTH RESEARCH DATA

English text only

85493

FOREWORD

"Data Protection in Transborder Flows of Health Research Data" addresses an issue of growing relevance raised by the rapid and simultaneous advances of information technologies and health sciences and technologies.

The issue relates to very different goals and interests: basic questions of human rights, the pursuit of scientific and technological progress, great medical needs and opportunities, but also considerable industrial and economic interests.

The question is, how to respect the right of individuals for privacy protection while at the same time gaining scientifically necessary access to personal data at the global level, in order to provide health benefits for society at large.

The present report goes back to March 1998 when the Working Group on Human-Health-Related Biotechnologies and the Working Party on Biotechnology of the OECD Committee for Scientific and Technological Policy agreed on a proposal to carry out a study on data protection issues in transborder flows of medical data. This agreement took into consideration that the OECD had already carried out considerable work on related issues such as privacy protection and transborder data flows. The OECD subsequently asked a leading international expert, Dr. William Lowrance, to review the key questions, indicate priorities and chart a course of action for the future, should governments be ready to continue work on this topic.

Dr. Lowrance's report was discussed and approved by the Working Group on Human-Health-Related Biotechnologies (17 May 1999) and the Working Party on Biotechnology (17 and 18 May 1999). National delegates appreciated the quality and timeliness of the report and recommended that it be made available to a larger public. The Committee for Scientific and Technological Policy subsequently agreed to its declassification.

This is why the OECD is releasing it now for wider circulation. This report is likely to influence many ongoing discussions. If it has not led to an immediate follow–up activity in the OECD, it is not for lack of interest by the Organisation. In fact, in spite of diverging interests and goals among some of the main stakeholders, the issue is too important to disappear from the international agenda. It may re-emerge in the OECD as well.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Computer-based health data systems; a wealth of databases; internationally networked data-transfer capabilities; telemedicine; electronic data-capture and electronic regulatory filing; and the coding, software, and hardware infrastructure to make all of them work – these technologies (which the report describes) are now on the verge of fulfilling their extraordinary promise, for research as well as for other purposes.

Health research has always transcended borders. Now the demand to transfer health data across national borders is increasing, in part because the informatics technologies make transfer more practical and useful. But such transfer will not occur fluently until a number of very difficult privacy and confidentiality issues are resolved. Confidentiality of health data continues to be demanded by the public, by health care providers, and by health researchers.

The fundamental challenge for health research is to respect individuals' privacy while at the same time pursuing justified access to personal data in order to provide health benefits for society.

In February 1999 an important Group-8 report, *Barriers to a Global Information Society for Health*, concluded that "protecting personal health information... is the most significant [barrier] at this point in time." The G-8 report's first recommendation was that:

> [E]ncouragement be given to the production of an international model contract or a Memorandum of Understanding, preferably including internationally acceptable guidelines, on data protection measures that would, particularly in the context of the EU Directive, be satisfactory in trans-national contracts to protect the confidentiality and security of personal health data.

Many organisations are working on the problems, especially on the more technical aspects. There is a pressing need for an organisation such as the OECD to take on an international leadership and co-ordinating role. The OECD would do well to build upon the Group-8 effort and the others that the present "Scoping Study" cites, and take initiative to help resolve some of the issues. Many technical standards organisations, the European Commission, the World Health Organization, and professional and trade organisations could be involved.

Probably an OECD project would focus on data used in health research, not on all health-related data. Taking advantage of OECD's international reach, presumably it would examine transborder data-flow, as opposed to data-flow within countries. It would be concerned with privacy and data protection, not just with the facilitation of data-flow. And it might encourage collaborative efforts between the public and private sectors on these issues.

For its basic ethical reference, the project would naturally have the widely respected OECD "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" and their many legal embodiments. The project could recognise and build upon the OECD's continuing work regarding encryption, authentication, and certification in electronic communications, the encouragement of fair data practices in electronic transactions, and other informatics and data protection matters.

Four tasks are suggested for the OECD project: a survey of needs and current efforts; a series of case studies; a survey of "practice" issues; and a review of data protection code and contract issues.

Suggested for consideration are case studies on: (a) international transfer of clinical trial data; (b) international regulatory filing of pharmaceutical data; (c) international exchanges of drug safety data; (d) international access to medical or public health databases; (e) selected EU health telematics experience; and (f) other transborder research data transfers.

An initiative to develop an international convention governing transborder flows of health research data might be considered.

NOTE DE SYNTHÈSE

Systèmes informatisés de données médicales, banques de données, réseaux internationaux de transmission de données, télémédecine, saisie et archivage électroniques de textes réglementaires, toutes ces technologies (décrites dans ce rapport), et les systèmes de codage, les logiciels et le matériel nécessaires à leur fonctionnement, sont en passe de remplir leurs extraordinaires promesses, que ce soit au service de la recherche ou d'autres activités.

La recherche médicale s'est toujours jouée des frontières. Aujourd'hui, la demande d'échange de données médicales entre les pays est plus forte que jamais, notamment parce que les technologies de l'information facilitent ces transferts. Toutefois, la circulation des données ne pourra être vraiment fluide que si un certain nombre de problèmes très complexes de protection de la vie privée et de confidentialité des données sont résolus. La confidentialité des données médicales est en effet l'une des exigences constamment exprimées par le public, les professionnels de santé et les chercheurs.

La difficulté consiste pour la recherche médicale à respecter la vie privée tout en obtenant l'accès à des données personnelles dont l'exploitation peut conduire à des avancées médicales utiles à l'ensemble de la société.

En février 1999, un important rapport du G-8 intitulé : «*Les obstacles à une société mondiale de l'information au service de la santé* » concluait que «la protection des données médicales personnelles… représente à ce jour le principal obstacle [à la diffusion de l'information]». La première recommandation de ce rapport préconisait :

> «[…] d'encourager la mise au point d'un modèle de contrat international, ou d'un protocole d'accord, contenant de préférence des lignes directrices applicables à l'échelle internationale, qui pourrait servir de référence en matière d'échanges de données entre les pays, eu égard notamment aux dispositions de la Directive de l'Union européenne, afin de garantir la confidentialité et la sécurité des données médicales personnelles. »

De nombreuses organisations travaillent sur ces questions, plus particulièrement sur les aspects techniques. Il devient indispensable qu'une organisation comme l'OCDE assure la coordination des efforts internationaux dans ce domaine. L'OCDE aurait intérêt à s'appuyer sur les travaux du G-8 et sur les autres travaux cités dans cette « Étude exploratoire » pour initier des actions destinées à résoudre certaines de ces questions. Des organisations de normalisation technique, la Commission européenne et l'Organisation mondiale de la santé, des organismes professionnels et commerciaux, pourraient être associés à ces actions.

L'OCDE pourrait lancer un projet qui porterait sur les données utilisées pour les besoins de la recherche médicale, et non pas les données médicales en général. Tirant parti de sa dimension internationale, l'Organisation pourrait se consacrer aux flux transfrontières de données plutôt qu'aux flux intranationaux, et étudier les questions de protection des données et de la vie privée sans se limiter aux moyens de faciliter les échanges de données. Elle pourrait aussi encourager les projets de collaboration entre les sphères publique et privée dans ce domaine.

En ce qui concerne la dimension éthique, le projet se référerait naturellement aux « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel » et aux nombreux textes juridiques qui s'en inspirent. Il s'inscrirait dans le droit fil des travaux que l'OCDE consacre en permanence à la cryptographie, l'authentification et la certification dans les communications électroniques, à la diffusion de bonnes pratiques en matière de transactions électroniques et à d'autres questions liées à la protection des données.

Le projet pourrait comporter quatre volets : un état des lieux des initiatives et des besoins actuels ; une série d'études de cas ; une étude sur les questions « pratiques » ; un examen des questions liées aux codes et contrats de protection des données.

Plusieurs thèmes sont suggérés pour les études de cas : (a) les transferts internationaux de données d'essais cliniques ; (b) l'archivage électronique de données pharmaceutiques à des fins réglementaires ; (c) les échanges internationaux de données sur la sécurité des médicaments ; (d) l'accès international aux banques de données médicales ou de santé publique ; (e) l'étude de quelques-uns des projets de recherche en télématique de santé financés par l'Union européenne ; (f) l'étude de quelques autres projets de recherche sur les flux transfrontières de données.

La mise au point d'une convention internationale régissant les flux transfrontières de données utiles à la recherche médicale est une autre initiative qui mérite d'être étudiée.

DATA PROTECTION IN TRANSBORDER FLOWS OF HEALTH RESEARCH DATA

THE CHALLENGES

Transfer of information among the many parties involved, and efficient use of information technologies, are essential in health research. Data – discrete pieces of information – are a core currency of health care and health research. Dependence on data will only increase; so will the demand to transfer data. To some extent, even the character of data being transferred is changing, as more complex genomic data are being moved, for instance, and as telemedicine practices grow.

In February 1999, an important Group-8 report, *Barriers to a Global Information Society for Health*, identified four major barriers – "protecting personal health information; data meanings and database navigation; ownership and legal accountability; and access to networking and messaging standards" – and emphasised that the first "is the most significant at this point in time."[1]

Included in that first barrier were issues of confidentiality, data protection, codes of ethics, encryption, authentication, and authorisation. The G-8 report's first recommendation was that:

> [E]ncouragement be given to the production of an international model contract or a Memorandum of Understanding, preferably including internationally acceptable guidelines, on data protection measures that would, particularly in the context of the EU Directive, be satisfactory in trans-national contracts to protect the confidentiality and security of personal health data.

"A world-wide unifying influence on both legislation and guidelines (of which there are many)," the report noted, "are the principles embedded in the OECD Guidelines."

As the rapporteur for the September 1997 Business–Government Forum at the OECD on Medical Information Networks and Technologies (MINTs) concluded:[2]

> [B]ecause the ultimate success of medical information technology depends on efforts by both government and industry, the OECD can play a critical role in bringing focus and attention to these issues. By using its analytic and fact-gathering capabilities, it could provide a comprehensive study of health-related information technology in the Member nations. Seeking new opportunities to co-ordinate and apply that technology should remain a priority of all Member states.

Personal privacy and medical confidentiality continue to be demanded by the public, by health care providers, and by health researchers. The public is very anxious over the erosion of medical confidentiality. In research, personal data must be very carefully safeguarded and treated with fairness to the data-subjects, the people to whom the data pertain. Many legal protections exist, but they may not be fully adequate to the health informatics future. (See discussion of the legal context, below.)

A wide range of impressive electronic technologies exist, or are coming into practicality, that can capture, manipulate, store, and transfer health data with great sophistication. Complex images, including moving images such as sonograms, can be processed. Rich databases can be amassed, and they can be accessed from afar. Telecommunications networks can move data internationally at reasonable cost. Data transfer taking advantage of all these technologies can not only increase efficiencies and reduce costs, but make new modes of health research possible.

But the potential of these technologies and procedures has not been fully realised yet.[3] The barriers include:

- Lack of internationally accepted technical standards for many of the technologies (including many software and coding systems).

- Uneven cultural acceptance of electronic media, and the related work practices, within many health care and health research institutions.

- The fact that until recently health care and payment, health law, and most health research involving personal data, have been, at broadest, restricted to being national-scale activities; and

- Serious difficulties and uncertainties over privacy and data protection.

As the informatics technologies are moved into routine use and data transfer increases, it will be essential to continue to safeguard privacy, and where new opportunities or threats arise regarding personal data, to renegotiate the terms – among institutions, and with "society" – under which data are handled and protected.

The fundamental challenge for health research is to respect individuals' privacy while at the same time pursuing justified access to personal data in order to provide health benefits for society.[4]

Health research has always transcended borders. But the enhanced informatics possibilities and new research demands, coming in this era of major reform in health care systems and revision in data protection regimes, are raising difficult international issues well worthy of the OECD's attention.

This "Scoping Study" will first sketch the data context and trends, health research purposes and approaches, and the legal context and issues. Then it will outline a series of tasks that the OECD project could beneficially pursue.

DATA CONTEXT AND TRENDS

Types of health related data

The large variety, volume, and diversity of uses of health related data are indicated by the following, very abbreviated, list.

- *Health care data* (basic medical and clinical patient records and the ancillary data linked to them, such as family history, laboratory, pathology, imaging, prescribing, pharmacy, interview, and therapy data). Almost all such data can be recorded in digital form and processed electronically.

- *Health care administrative data* (eligibility, admissions and discharge data; routine operational data; and insurance and financial transactional data). For such purposes as management, payment, and auditing, these are processed and stored in many institutions beyond clinical settings.

- *Population-based public health data* (birth, death, abortion, and other vital records; screening and disease-monitoring data; many health-services data; and registries concerning such matters as infectious diseases, cancer, birth defects, vaccination, implanted medical devices, and genomics).

- *Primary research and technical regulatory data* (basic research data; data collected in health services, outcomes, economics, and other studies; and clinical trial, drug safety surveillance, and other data generated to support product and service development and market authorisation).

Research is, of course, performed on data collected specifically for the purpose, but research can also be performed on any health related data. Detailed patient-level cost data may, for example, be studied in economic analyses. Thus "health research data" is an elusive notion, and generally means "data (of whatever kind, from whatever source) being used for health research purposes."

As managed care and other institutions perform studies internally, as public health authorities conduct disease monitoring and other surveillance, as marketers perform analyses, even "research" may not be easy to define. In practice, most research can be so identified, but there are activities at the margins that may, in legal contexts, be of disputable status as research.

One more definitional issue. Distinction may be made between "health" and "medical," with "health" referring to a person's physical and mental state, and "medical" referring to interaction with licensed medical providers and certified medical institutions. In this "Scoping Study", most references to "health data," will include not only medical data but also many other kinds of personal data.

Advances in health informatics

As will be sketched below, a robust array of data technologies is now being applied in health care and research. Technically it knows no national bounds. Anywhere electrons can be channelled; health data can be transferred. The trends include the following. They are occurring locally first, but they can be extended to an international scale.

Research itself makes use of all of these technologies as it handles data, and it analyses the data that these technologies carry from health care, public health, and administrative sources.

Electronic health care records and systems

More and more, health care services are being computerised; and more and more, data are being transferred electronically. Most health care activities in the OECD countries are at least partially computerised now.

The future ideal, from the "informatics true believers" perspective, comprises patient-level health care record systems that are: comprehensive (as opposed to scattered by incidents, specialties, or institutional settings); cumulative throughout lifetimes; standardised as to data coding and formatting (to be universally interpretable); networked and inter-operable (to allow effective data transfer among diverse units and data systems); and secure (to prevent their being intercepted or corrupted, and to control access).

The European Commission has invested heavily in the "Good European Health Record" and related health telematics projects. In the UK, the National Health Service has been promoting the use of information technology and the nation-wide "NHSnet," but at the same time has been very much concerned about

confidentiality and data protection.[5] In Germany, many medical telematics components are in operation, and many initiatives are underway, but a unified strategy has been slow to coalesce, in part because of data protection concerns.[6]

In 1997, a committee of the Institute of Medicine (USA) identified five objectives that "computer-based" medical record systems must meet:[7]

> [F]irst, future patient records must support patient care and improve its quality. Second, they must enhance the productivity of health care professionals and reduce the administrative and labor costs associated with health care delivery and financing. Third, they must support clinical and health services research. Fourth, they must be able to accommodate future developments in health care technology, policy, management, and finance. Fifth – and the committee placed great emphasis on this – patient confidentiality must be maintained while these objectives are being met.

The same should be required of health informatics systems generally. It is not only "doctors' files" (for short) that are being computerised. Prescribing and pharmacy dispensing records are, too, as are all manner of data from laboratory analyses, medical imaging, speech and physical therapy, optician services, genetic screening, psychological counselling, smoking or alcoholism treatment, and other activities.

Microchip smartcard systems

Memory cards can store personal identification, data about insurance coverage, emergency medical data (blood type, allergies, and so on), and, potentially, many other health-related data. Hundreds of millions of such cards are now in use by consumers and health care providers, especially in Europe. Mostly they are used as high-tech identification cards. Some cards are specialised, carrying data about diabetes or epilepsy status, for example. Card systems can be used as an adjunct to health research.

Increasingly, smartcards are being required as a condition for payment. In Germany, some 85 million health-insurance cards (*Versichertencarte*) are in use. In France there is a move toward requiring universal *Sesame-Vitale* cards to authorise reimbursement by the social security system. But in both countries the systems are surrounded by data protection controversy.

Telehealth, telemedicine

"*Tele*" – at a distance. A impressive array of methods are being developed for using telecommunications in delivering health care and performing research. Pioneered in part to help provide care to rural and distant military populations, these systems are quickly moving into general application. They can facilitate consultations by transferring images among specialists, for instance, or send a prescription to a pharmacy, or support self-care and home care. They can be as useful within a city as at long distances. But they offer unique possibilities for health communication at long distances.[8] A great many different hardware and software technologies are involved, and their development is strongly market-driven.[9] Again, standardisation, or at least interchangeability, is a major challenge in their diffusion.

Because most laws governing medical confidentiality are local (at broadest, national), special arrangements must be made to preserve confidentiality and patient rights as data are transferred among medical jurisdictions. This is an especially pressing concern in the consolidation of health care in Europe. Telemedicine, too, raises crucial issues of message authentication and security.

In the future, as is beginning to occur now, clinical-trial and other data will be "captured" electronically at clinical sites and transmitted directly to sponsoring companies; and those companies will electronically submit data to drug regulatory agencies.[10] Many of the data protection issues will closely resemble those in telemedicine.

Health-related databases

Most of the data that move through systems become deposited in databases. Many databases are simply storage archives. But some are organised in sophisticated ways, hold data in standardised form, and allow flexible searching for multiple purposes.

Health-related databases are growing rapidly in scale and power, and demand for access to them is rising concomitantly. These databases may be organised by institution (hospital, for instance), demographics (Saskatchewan), illness (asthma), treatment (polio vaccination), service (pathology), payment, or other themes. Many contain sensitive records on millions or even tens of millions of people's health experience.

Often databases are useful not only to the organisations that manage them for their internal purposes, but also to others, including researchers. Through telecommunications, databases can potentially be accessed from any distance. Many ethical and legal issues surround database research.

Internet communications with the public

The Internet is increasingly being used for health purposes – to inform, consult, survey, advertise, sell products and services, and communicate with patients in disease management and home care.

The Internet and various intranets are used to transfer research data. And secondary research is performed on data initially collected via the Internet for purposes such as those just listed.[11] Sensitive issues of data protection, including data-subject consent, message authentication, and security, abound.

Health research purposes and approaches

Health research is pursued for countless particular purposes. It proceeds via many technical approaches. And it uses whatever data it can bring to bear on the questions. Research is conducted:[12]

- To advance basic biomedical science
- To know patterns of health, disease, and disability
- To reduce public health threats
- To understand utilisation of health care
- To evaluate and improve practices
- To make effective innovations
- To analyse economic factors

- To appraise markets.

Research now is delineating patterns of health, disease, and health care with a power never possible before. It is revealing causes. It is evaluating "what works," with what benefits, for whom, in what circumstances, why, at what costs (broadly defined), and with what cost-effectiveness. And as the news media and stock markets indicate every day, it is continuing to develop marvellous new possibilities for promoting health and coping with illness and disability. All of these kinds of research are becoming more international in character, and they need to be able to allow data transfer across national borders.

Research can use all of the types of data and informatics systems mentioned in the preceding sections. A prominent research desire is to be able, in future, to "tap into" data-streams, in order to monitor health care practices, outcomes, and economics; conduct public health surveillance; analyse the changing demands and markets for prevention and care; and so on. Another research desire is to have fuller access to databases, and to interlink data from diverse databases so as to assemble richer dossiers on issues under study.

LEGAL CONTEXT AND ISSUES

Legal background

The classic protection of medical privacy, of course, is the "medical secrecy" compact, originating with the Hippocratic ideals, that is embodied in the licensing of physicians and other health care professionals, and that is embraced in most health care contracts and medical confidentiality laws. Despite considerable erosion in recent years, this confidentiality undertaking still has validity, is thought to encourage patients to enter fully into healthcare and research transactions, and is valued by the public and by health care providers. All OECD nations have laws protecting medical confidentiality to varying degrees.

For consent and confidentiality in research, the seminal instrument is the World Medical Association's "Declaration of Helsinki: Recommendations Guiding Medical Doctors in Biomedical Research Involving Human Subjects."[13] Most countries now have strong, detailed regulations governing research on human subjects. Such regulations take account of risks to subjects, and are based around informed consent by data-subjects and promises of protection by researchers. Confidentiality is usually covered, at least nominally.[14] Some of the traditional protections may be inadequate against the changes surveyed in this report.

For personal data generally, fundamental principles were set forth in the 1980 OECD "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."[15] These principles were then embodied in the 1981 Council of Europe "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," which has now been ratified by 20 nations.[16] The Convention distinguished a category, "sensitive data," and cited medical data as an example.

The OECD principles address:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation

- Security safeguards
- Openness
- Individual participation
- Accountability.

The OECD principles have become the essence of most of the world's privacy and data protection laws.[17] Where such laws do not exist or apply fully, the principles are echoed in many guidances for voluntary private sector practice, such as the Australian "National Principles for the Fair Handling of Personal Information" and the "Privacy Principles" of the US National Information Infrastructure.[18] And they are the legal core of the European Union (EU) Data Protection Directive, which, because it is driving much current change and raising broad issues, will be discussed in some detail here.

The current legal sea-change

In 1995 the EU adopted the "Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data."[19] This framework directive establishes an elaborate set of principles, procedures, and penalties on the handling of personal data.

The deadline for implementing the principles of the Directive into the 15 EU Member States' national laws was October 25, 1998. Although, no surprise, schedules have slipped, all of the Member States are moving toward compliance by adapting their laws and subsidiary regulations.[20] Other countries in the European Economic Area (such as Norway) are bringing their laws into analogy, as are Central European countries (such as Hungary) that aspire to joining the EU.

The Directive covers all personal data, and it construes identifiability broadly (Article 2.a):

> [A]n identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

For health research, identifiability is an important issue, since many of the data are highly specific to individuals, and because it may be necessary to preserve the ability to trace back to the original records, or even the data-subjects, to verify data, obtain additional information, eliminate duplicate cases, or follow up over time.

The Directive focuses on data processing rather than on data ownership, thereby relating data handling to consequences for the data-subjects.[21] It defines "processing" as being, in effect, all situations in which there may be an opportunity for handling or becoming aware of data (Article 2.b):

> [Processing is] any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The Directive addresses data quality, purpose limitation, data-subject rights (to inspect records about oneself, object to processing, and so on), and many other matters, and establishes judicial remedies for

breach. It is more restrictive on "sensitive data," which it defines as including racial and ethnic data and "data on health or sex life." Consent of data-subjects is a pivotal notion.

The EU Directive provides little guidance on how health data, in particular, are to be treated, beyond noting, importantly (in Article 8), that Member States may provide for exemptions:

> [W]here processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

But it does not define these purposes, so there is uncertainty over which of the many health research activities described earlier might be eligible for special dispensation by EU Member State laws. As a minimum, it is expected that processing of personal data to comply with public health laws, such as in infectious disease reporting and drug safety surveillance, will be conceded special status, with data protection still required but perhaps some obligations of consent and so on waived. The OECD might be able to help bring about some of the needed clarification.

The Directive (Article 25) stipulates that personal data may not be transferred from an EU country to non-EU recipient country unless the protections in the recipient country are deemed to afford "adequate levels of protection."[22] High-level diplomatic negotiations are proceeding currently on how "adequacy" is to be interpreted, especially for non-EU countries (such as the USA and Japan) that do not have omnibus data protection laws and a governmental enforcement apparatus.

Non-EU countries are working to adapt their laws and other social controls, such as industry self-regulatory regimens, so that they can continue to receive personal data from EU countries. A later section of this report will discuss codes of conduct and contracts as mechanisms relating to data transfer.

In 1996, the USA adopted the Health Insurance Portability and Accountability Act (HIPAA). Among many other things, the Act requires the Secretary of Health and Human Services (HHS) to adopt standards for electronic financial and administrative transactions, which are being drafted now. And it requires that if no legislation on standards for the protection of confidentiality of health information used in health claims transactions is enacted by August 1999, the HHS Secretary must, within six months, then issue regulations.

With the HIPAA and other driving forces exerting pressure, the US Congress is considering the adoption of a national medical confidentiality law. Having such a law (or regulations) in place surely would be a reassurance as to the "adequacy" of protection for health data transferred from EU sources.

In 1997, the Council of Europe, a body of 39 countries that includes all of the EU countries and many of the OECD countries, adopted a detailed "Recommendation on the Protection of Medical Data."[23] This Recommendation does not appear to have been implemented yet, but it may well become important. Among other things, it describes criteria for the secondary use of medical data.

All of this activity intersects with the vigorous international debate over self-regulation and external regulation of the Internet and electronic commerce (again, an arena in which the OECD is playing prominent roles).

The cross-cutting concern is how data protection can be guaranteed – ethically, legally, and technically – as health data are moved across national jurisdictions (and in some cases, at the same time across provincial jurisdictions, such as those of the German Länder, the US States, or the Canadian Provinces, which may impose data protection requirements beyond the national ones).

As will be discussed in turn, below, at least four possible tasks can be considered for the OECD project:

- Survey of needs and current efforts
- Case studies
- Survey of "practice" issues
- Review of codes and contracts**.**

TASK: SURVEY OF NEEDS AND CURRENT EFFORTS

Proceeding via small expert workshops, interviews, and input from the Business and Industry Advisory Committee to the OECD (BIAC) and specialised organisations, the project might survey the data protection issues that must be resolved in order to foster transborder transfer of health research data. This would elaborate upon the issues raised by this "Scoping Study" and others that might be identified.

Complementarily, the project might inventory the work that is being sponsored or carried out by national governments, intergovernmental bodies (such as the European Union and the Council of Europe), international organisations (the International Standards Organization and the World Health Organization), and many professional societies and sectoral organisations.

TASK: CASE STUDIES

Because a number of successful, if specialised, transborder data transfers are now regularly being conducted, and because some pilot programmes have had time to run, the OECD project could provide an important practical service by preparing brief case studies and drawing out "lessons being learned", and identifying issues that need to be attended to. The case studies should be succinct. A few anecdotes from the MINTs Workshop (on managed care databases, for instance, or health smartcards) might be good cases for follow-up. The following are examples of cases that might be reviewed. (*As yet, no organisation has been asked about or assented to such case studies; they are sketched here to be indicative.*)

Possible case study A: International transfer of clinical trial data

Clinical trial data – massive amounts of diverse, detailed, highly personal data – are transferred among investigators, sponsoring companies and their affiliates and service contractors, and government agencies. Large volumes of such transfers occur routinely, on a global scale.[24]

These transfers are generally considered a success in transferring data while protecting data-subjects. Internationally respected practices are employed, data-subject informed consent is required, ethics review boards supervise the protocols, and transfers are made under reasonable security. Reviewing how clinical trials data are handled in transfer should illustrate "high end" practices.

Possible case study B: International electronic regulatory filing of pharmaceutical data for marketing authorisation and related purposes

Proceeding under elaborate Guidelines from the International Conference on Harmonization, developed jointly by the pharmaceutical industry and drug regulatory authorities of Japan, Europe, and the USA, these are efforts to submit the equivalent of millions of pages of complex data electronically instead of via

paper, thereby securing many advantages in transfer, storage, searching, analysis, and other processing.[25] (Typically an initial new-drug application fills several million paper pages with technical detail, and then the dossier grows.)

Some large-scale pilot filings, conducted in parallel electronically and via paper, have been conducted. The advantages and difficulties of electronic submission could profitably be summarised, in part to indicate considerations for other kinds of health-related transborder filings.

Possible case study C: International exchanges of drug safety data

A range of projects are proceeding under the aegis of the EU DG-III to develop a robust telematics infrastructure to support pharmaceutical R&D and public health regulation. Communicating via the "EudraNet" and working within the "EudraWatch" pharmacovigilance system, the European Medicines Evaluation Agency (EMEA) electronically assembles, among other data, adverse event reports from the EU countries' drug regulatory authorities.[26]

The World Health Organization (WHO) Collaborating Centre for International Drug Monitoring in Uppsala collects reports from 53 countries, compiles them into a sophisticated database, and searches the database to pick up early signals of possible drug safety problems.[27]

The extensive technical progress being worked through in these programmes, and the handling of such issues as personal identifiability of the data, could be described with the aim of drawing out lessons for the development of future international public health data systems.

Possible case study D: International access to medical or public health databases

Database research brings up complex issues of consent, de-identification of data, security, contractual assurances, and other protections.[28] A number of major health databases are depended upon for important research from outside the country of data origin. Many others would be used if the confidentiality, security, and legal problems were solved.

To mention one example, the UK General Purpose Research Database (GPRD), assembles clinicians' ongoing data on a broad sample of some six million British patients. To researchers, this is a treasure. Usually, intermediate "stripping" operations are performed to remove personally identifying data before the data are shown to researchers. The data are routinely transferred to specifically licensed, fee-paying researchers outside the UK.

It is important to recognise that with databases, access-at-distance even if only temporarily may on legal grounds amount to "processing" (in the sense of the EU Directive) or "transfer."

A very useful service by the OECD would be to survey current policies and practices as regards the ethical, legal, and technical conditions for health database access/transfer in research.

Possible case study E: Selected EU health telematics experience

In its Fourth R&D Framework Programme, 1994–1998, the European Commission's Directorate-General XIII has sponsored some 130 health telematics projects. These include projects on smartcards, a data network in a cross-border regional renal dialysis programme, telematics support for emergency medical

services, and a complex oncology network. Many of the technologies are moving into commercialisation and use now. Many will have transborder applicability, even if initially only within the EU.[29]

It would be highly desirable to review a few of these developments, perhaps ideally some real field applications, with respect to data protection in transborder data flow, even if research is not the primary purpose of the data transfers. This should be performed in close co-ordination with DG-XIII and other parts of the Commission, and would be a natural joint OECD–EC effort.

Possible case study F: Other transborder research data transfers

In co-operation with Member governments and BIAC, other research projects and public health programmes that involve the transfer of personal data could be identified. Many such projects proceed routinely. Usually precautions are made to obtain consent, and perhaps to de-identify the data before they are transferred from the source country.

For projects for which national laws do not provide sufficient auspices, ad hoc binational or other agreements often are entered into. It would be useful to identify the effective features of such research treaties or contracts, and discuss their practicality and enforceability. This might even contribute to the designing of a generic international convention on such transfers.

TASK: SURVEY OF "PRACTICE" ISSUES

The following aspects of practice – the day-to-day craft of data protection— deserve serious review and attention. They are the specifics of laws, regulations, data transfer contracts, and codes of practice. And they are the specifics of research institutions' Standard Operating Practices, and of the criteria that ethics review boards apply. When these matters are tended to properly, usually data are allowed to flow. These practice issues will arise in any case studies, but they might be surveyed as cross-cutting themes.

Handling of data-subject identifiability

For any study, researchers must decide whether data must be used in personally identified form (that is, associated with individuals), or whether non-identified data will suffice.

Most health data begin as identified data. But they can be de-identified either:

(a) Irreversibly, by discarding identifying information, or by aggregating (averaging) sets of data; or

(b) Reversibly, by removing identifying information and assigning an arbitrary pseudonym (usually a number) connecting the substantive data with the identifiers ("key-coding"), and safeguarding the key separately.

Indirect identifiability is always a concern. De-identification requires not only removing all overt identifiers (name, address, birth date, national health number, etc.), but also removing, masking, or blurring data that might contribute to indirect, deductive identification (such as spouse's name, or accident information, or a variety of other distinguishing data).

Irreversible de-identification is not always possible or desirable. A number of practical and ethical issues can arise. In many health research (and related regulatory) investigations there is an essential need to maintain the ability to follow, or to trace back to, the data-subjects or other records about them.[30]

Experiences with various solutions being tried – such as arranging for trusted external parties to remove identifying data, and/or to safeguard the identifiers or the "key" that can reconnect them to the case data deserve review. So do the ways various public health regulations address identifiability.

Data-subject consent

Central to all data protection regimens is consent. It is not obvious how the OECD project could contribute regarding consent, except to address it in case studies. As a minimum, it must be recognised that consent is a crucial issue, but that fully informed, freely granted, specific consent for specific purposes is a difficult ideal to achieve. When consent is not obtainable, carefully de-identifying the data and committing it to specified safeguards may allow the research to be conducted. This is especially an issue in secondary research.

Secondary research use of data

Much research performed on transferred data is secondary research – re-use of data, for purposes either similar to, or different from, the purposes for which the data were originally collected. Judgments as to whether a purpose is "similar" to the original purpose (and thus meets the OECD "purpose specification" and "use limitation" principles) can be contentious. So can judgments as to whether re-consent should be sought from the data-subjects.

The further the "distance" of a new use from the original point or time of data collection, or from the data-subject, probably the more difficult it is to guarantee that data-subject rights are respected. Much needs to be done on secondary use.

Safeguards and security

Data security in general is a very broad topic, and the security issues in health research, though crucially important, are not very different from those in other endeavours. But surely there are aspects of digital signatures, certification authorities, encryption, and the like, on which the OECD, because of its extensive experience and ongoing involvement, would be able to make contributions.

Preservation of data-subject rights

How can the legal rights of data-subjects – such as those embodied in the EU Directive and embedded in so many laws – be trailed along and enforced as data are transferred transborder, and then perhaps transferred further? How can members of the public pursue inquiries concerning data about themselves, or seek amendments or liabilities? The answers are uncertain. Again, the OECD has much relevant experience to bring to the discussion.

TASK: REVIEW OF CODES AND CONTRACTS

Codes and contracts are being explored for assuring data protection, and they have relevance for transborder transfer. Although these instruments are not new, new legal burdens are being laid on them.

Professional and sectoral codes of practice

Health researchers have long relied on communal codes and guidelines, which tend to hybridise "good public health" with "good science" considerations. The EU Directive encourages the endorsement of codes of conduct as elements of self-regulation (Article 27), and therefore also as factors that might dispose to findings of "adequate protection" in transborder transfer.

Japan has responded to the EU Directive by publishing, in March 1997, "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector," the implementation of which, sector by sector, is being supervised by the Ministry of International Trade and Industry (MITI). An independent body chartered by MITI is certifying compliance by companies.

In The Netherlands, the Council for Medical Research, a professional body, maintains a voluntary "Code of Conduct" on privacy and research, which has been approved by the national Data Protection Commission (*Registratiekamer*). Cases are still subject to supervision by the Commission, but the generally approved practice is clear.[31] Recently, the research councils of Canada, which disburse federal funds, adopted a policy covering such matters as informed consent and confidentiality, and stated that they "will consider funding only to individuals or institutions which certify compliance with this policy."[32]

The promise of such quasi-voluntary codes is that they can guide complex endeavours and establish uniform practices. Always a question about such codes is whether conformance can be verified and enforced. The Dutch and Canadian codes mentioned above are examples of codes reinforced by external incentives (scrutiny by the data protection authority, and eligibility for funding).

Several industry organisations, such as the European Federation of Pharmaceutical Industries and Associations (EFPIA), have been considering whether codes of practice will be useful. But there have been hesitations, concerning: whether a code can be drafted that is specific enough to guide practice, yet be sufficiently broad and flexible to be applied in a diversity of companies, research programmes, and legal jurisdictions; whether transparency and enforcement can be assured to the public; and whether the adoption of a code would help secure EU exemptions, or special dispensations, for the specialised data processing that pharmaceutical firms conduct.

Now, as should be expected, the provisions of many guidelines, codes of practice, recommendations, and regulations are converging. An OECD project could help summarise the common themes. It might also be able to help consolidate the guidance.

Data transfer contracts

The EU Directive (Article 26.2) suggests that contractual undertakings may serve to guarantee that data being transferred from EU to non-EU countries will be protected.[33] Contracts might be just as useful in transfers between two non-EU countries.

The proposition is that a data processor intending to transfer data to another processor should do so under a contract with the data recipient, specifying that the recipient will maintain appropriate safeguards and

security, limit further disclosure, preserve the data-subject's rights, and agree to liabilities if the contract is breached. Some practical experience with such contracts has accrued, but under somewhat unusual circumstances.

The Council of Europe, the International Chamber of Commerce, the non-profit Privacy and American Business organisation, and other bodies, have been developing model contracts. How effective and efficient such generic contractual clauses will be when applied broadly is unclear.

One troublesome set of issues has to do with how effectively, in a practical sense, contracts can preserve data-subjects' rights as data are transferred outside the country in which the subjects entered into an agreement with the data collector.

An obvious question is whether liabilities under such contracts can be enforced.

The OECD has accrued much experience with data transfer contract issues, especially regarding the use of contracts in on-line commerce. Identifying the advantages and disadvantages, and summarising any evaluations and current directions, of data protection codes and contracts – in particular as they might foster transborder flow of data in health research – would be a valuable service by the OECD.

RANGE OF A POSSIBLE OECD PROJECT

An OECD project would probably focus on data used in health research, not on all health-related data. Taking advantage of the OECD's international reach, it would presumably examine transborder data-flow, as opposed to data-flow within countries. It would be concerned with privacy and data protection, not just with the facilitation of data-flow. And it might encourage collaborative efforts between the public and private sectors on these issues.

As its basic ethical reference, the project would naturally have the OECD "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" and their many legal embodiments.

The project could recognise and build upon the OECD's continuing work regarding encryption (encoding of messages for secure transmission), digital signatures and other techniques of authentication and certification in electronic communications, the encouragement of fair data practices and trustworthiness in electronic transactions, and other informatics and data protection matters.

While the project should fit within the context of protection of personal data generally, its special mandate would be to address issues that are specific to health research.

(A note on scope. This preliminary study has focused on health research data. But the OECD may decide to cover health data generally. Often it is difficult to distinguish – conceptually, cybernetically, legally – "research data" from other categories of data. It can even be difficult to distinguish "research purpose" from health care or public health purpose. The issues identified in the present study are important, susceptible of being analysed, and indicate the parameters of the larger issues. Probably in its initial phase an OECD project would want to pursue the research data issues.)

WHY AN OECD PROJECT?

Computer-based health data systems; a wealth of databases; internationally networked data-transfer capabilities; telemedicine; electronic data-capture, and electronic regulatory filing; and the coding,

software, and hardware infrastructure to make all of them work – all of these data-handling technologies are on the verge of fulfilling their extraordinary promise.

But the endeavours suffer, in some ways, from being "common" problems: although everybody will benefit once these technologies are applied, far fewer are willing to invest in nourishing the development, financially and otherwise. Meanwhile, various proprietary firms and standards groups are proceeding entrepreneurially. The very difficult privacy and confidentiality issues, and to a lesser extent the security and authentication issues, have been less successfully attended to so far than the technological advances.

Why the OECD? There are many advantages in the OECD's taking on a leadership and co-ordinating role.

- The OECD works closely with its Member governments and their ministries and agencies, of course; and in this project, as it does in others, it could work closely with the private sector as well. Part of the impetus for this "Scoping Study" was its being recommended by the Business and Industry Advisory Committee (BIAC). The health care and telematics industries are very much concerned to have these issues resolved. Thus the OECD should be able to achieve the necessary collaboration between the public and private sectors.

- Although many organisations are working on health informatics, or on data protection, or on research strategies, leadership and co-ordination are needed. This report has outlined a variety of survey, stock-taking, case study, and "brokering" possibilities.

  The international and European technical standards organisations and programmes could be involved, and their technical work deferred to. What the OECD probably would focus on are the more social and legal data protection and transfer aspects.

  The EU and its Commission could be involved. These issues are of concern to DG-III (health care industry and its regulation), DG-XII (research and development), DG-XIII (telematics applications to health), and DG-XV (data protection and the Directive).

  The World Health Organization also could be involved, to take advantage of its global health experience and take into account its global concerns.

- Principles, such as the OECD data protection principles, are less the question now than their application to practice. The case studies such as those proposed, for which the OECD could provide practical auspices, should be very illuminating at this stage in the issues' evolution.

- The OECD would do well to build upon the Group-8 effort and the other efforts that the present "Scoping Study" has cited, and take initiative to help resolve some of the issues. An OECD project could help foster the movement toward internationally consistent "rules." An initiative to develop an international convention governing transborder flows of health research data might be considered.

- The Secretary-General has affirmed that the Organisation will give priority to health policy and economics. An OECD project on transborder flow of health research data would mesh well with, and be able to take advantage of, ongoing OECD work under both the Directorate for Science, Technology and Industry (DSTI) and its Committee for Information, Computer and Communication Policy (ICCP).

APPENDIX 1

"Basic principles of national application" in the OECD "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (September 23, 1980*)*

***Collection limitation principle*.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data-subject.

Data quality principle. Personal data shall be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose specification principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and their subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use limitation principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the preceding paragraph] except: (a) with the consent of the data-subject; or (b) by the authority of law.

Security safeguards principle. Personal data shall be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle. An individual should have the right: (a) to obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

APPENDIX 2

Excerpts from the EU Data Protection Directive (95/46/EC) regarding transfer of personal data from EU countries to non-EU countries[34]

Article 25.1

The Member States shall provide that the transfer to a third country [i.e., non-EU country, *note added*] of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Article 25.2

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Article 26.1

[M]ember States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25.2 may take place on condition that:

(a) The data subject has given his consent unambiguously to the proposed transfer; or

(b) The transfer is necessary for the performance of a contract between the data subject and the controller ... ; or

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) The transfer is necessary or legally required on important public interest grounds ...

Article 26.2

Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25.2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

NOTES

1 Project G8-Enable, *Barriers to a Global Information Society for Health* (IOS Press, Amsterdam, February 1999); available on the Internet at <http://www.ehto.be/sp5>. The G-8 members are Canada, France, Germany, Italy, Japan, Russia, the UK, and the USA; Australia also participated in the project.

2 Business and Industry Advisory Committee to the OECD (BIAC), Daniel Casse, rapporteur, *Report on the Business–Government Forum on Medical Information Networks and Technologies, Paris, September 17-18, 1997*; available from BIAC, 13-15 Chaussée de la Muette, F-75016 Paris. (That Forum was chaired by the current author.)

3 Project G8-Enable, as cited in note 1.

4 William W. Lowrance, *Privacy and Health Research: A Report to the US Secretary of Health and Human Services* (US Department of Health and Human Services, Washington, DC, May 1997); available on the Internet at <aspe.os.dhhs.gov/datacncl/phr.htm>.

5 National Health Service, *Information for Health: An Information Strategy for the Modern NHS 1998–2005*; summary available on the Internet at <http://www.nhsia.nhs.uk/strategy/full/1.htm>.

6 Forum INFO 2000, Schlussbericht der Arbeitsgruppe 7, *Telematic-Anwendungen in Gesundheits-wesen—Nutzungsfelder, Verbesserungspotentiale und Handlungsempfehlungen*, Schriftenreihe des Bundesministeriums für Gesundheit, Band 105 (Nomos-Verlag, Baden-Baden, 1998).

7 Institute of Medicine, Richard S. Dick, Elaine B. Steen, and Don E. Detmer, editors, *The Computer-Based Patient Record: An Essential Technology for Health Care*, Revised Edition, p. 94 (National Academy Press, Washington, DC, 1997).

8 Critiques and case studies were presented in Institute of Medicine, Committee on Evaluating Clinical Applications of Telemedicine, Marilyn J. Field, editor, *Telemedicine: A Guide to Assessing Telecommunications in Health Care* (National Academy Press, Washington, DC, 1996).

9 A wide range of technologies has been under development since 1994 in the health care telematics programme of EU Directorate XIII. See *4th Research & Development Framework Programme 1994-1998, '97 Healthcare Telematics*: vol. 1, *General Overview;* vol. 2, *Compendium of Projects* (DG-XIII C.4, B-1160 Brussels, 1998).

10 Amy J. Lampe and John M. Weiler, "Data capture from the sponsors' and investigators' perspectives: Balancing quality, speed, and cost," *Drug Information Journal 32*, 871-886 (1998).

11 The National Research Council (USA) is currently conducting a study, "Enhancing the Internet for Medical Applications: Technical Requirements and Implementation Strategies"; information is available on the Internet at <www4.nas.edu/webcr.nsf/projectscopedisplay/cstb-L-98-03-a>.

12 These purposes are discussed in this author's report cited in note 4, on pp. 21–31.

13 World Medical Association, "Declaration of Helsinki," latest revision 1989; available on the Internet at <www.ncgr.org/gpi/odyssey/privacy/heldec.html>.

14 In the USA, for instance, a uniform "Federal Policy for the Protection of Human Subjects," generally referred to as the "Common Rule," applies in 17 departments' and agencies' jurisdictions. It appears at *45 Code of Federal Regulations 46*, subpart A. The Common Rule was published in *Federal Register 56*,

28002-28032 (1991). The Rule addresses privacy risks and protections, but does not provide detailed guidance.

15 OECD, *Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); available on the Internet at <www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm>. The principles are provided as *Appendix 1* to the present report.

16 *European Treaty Series No. 108* (January 28, 1981); available on the Internet at <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>.

17 Examples of such laws include, for instance, the French *Loi relative à l'informatique, aux fichiers et aux libertés*, the German *Bundesdatenschutzgesetz*, the Hong Kong Personal Data (Privacy) Ordinance, the Swedish *Datalagen*, and the UK Data Protection Act. These laws are administered by independent commissions or commissioners having enforcement powers.

18 Office of the Privacy Commissioner of Australia, "National Principles for the Fair Handling of Personal Information," revised version with guidance notes (January 1999); available on the Internet at <http://www.privacy.gov.au/private/index.html>. U.S. Information Infrastructure Task Force, "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information" (June 6, 1995), available on the Internet at <www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

19 Directive (95/46/EC); available on the Internet at <http://www.europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm>.

20 EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Second Annual Report* (November 30, 1998); available on the Internet at <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp14en.htm>.

21 Ownership can be an issue, but most data protection laws focus on how data are handled, how the rights of data-subjects are respected, and how data-subjects might be affected, without regard to data ownership. "Ownership" of medical data can be an elusive notion.

22 Article 25 is provided in *Appendix 2* to the present report.

23 Council of Europe, "Recommendation of the Committee of Ministers to Member States on the Protection of Medical Data," No. R (97) 5 (February 13, 1997); available on the Internet at <www.coe.fr/dataprotection/rec/r(97)5e.htm>.

24 A description of an unnamed pharmaceutical company's transfers of clinical trial data appeared in Charles D. Raab, Colin J. Bennett, Robert M. Gellman, and Nigel Waters, "Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer" (EC Tender No. XV/97/18/D, September 1998); available on the Internet at <europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm>.

25 Mervyn Mitchard, editor, *Electronic Communication Technologies: A Practical Guide for Healthcare Manufacturers* (Interpharm Press, Inc., Buffalo Grove, Illinois, 1998).

26 A description of the DG-III E.3 telematics programme in pharmaceuticals is available on the Internet at <http://dg3.eudra.org/telemat/index.htm>.

27 Sten Olsson, "The role of the WHO Programme on International Monitoring in coordinating worldwide drug safety efforts," *Drug Safety 19*, No.1, 1-10 (1998).

[28] International Society for Pharmacoepidemiology (ISPE), "Data privacy, medical record confidentiality, and research in the interest of public health," as amended August 1998 (ISPE, 2000 L Street NW, Suite 200, Washington, DC 20036); available on the Internet at <www.pharmacoepi.org>.

[29] The DG-XIII programme was cited in note 9.

[30] For discussion of reasons for retaining identifiability in health research, see this author's report as cited in note 4, p. 36.

[31] Raad voor Gezondheidsonderzoek, *Gedragscode Gezondheidsonderzoek voorgelegd aan de Registratiekamer* (RGO, Postbus 9517, NL-2590 Den Haag).

[32] Medical Research Council of Canada, Natural Sciences and Engineering Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*; available on the Internet at <http://www.mrc.gc.ca/publications/publications.html>.

[33] An excerpt from Article 26 regarding contracts is provided in *Appendix 2* to the present report.

[34] The Directive was cited in note 19.