GenEditorial

EDITORIAL ON THE ETHICAL, LEGAL AND SOCIAL ISSUES OF HUMAN GENETICS

(2006) 4:1 *GenEdit,* 1-8

THE LEGAL FRAMING OF COMPUTERIZED PROCESSING OF HEALTH DATA : A EUROPEAN AND CANADIAN PERSPECTIVE

Cynthia Chassigneux[1], Pierre Trudel[1], Bartha Maria Knoppers[1]

The use of information and communication technologies in the health and social service sectors, and the development of multi-centred and international research networks present many benefits for society: for example, better follow-up on an individual's states of health, better quality of care, better control of expenses, and better communication between healthcare professionals. However, this approach raises issues relative to the protection of privacy: more specifically, to the processing of individual health information.

This data is defined as sensitive, notably by the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [1] (henceforth "Convention n°108") and the *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*[2] (henceforth "Directive 95/46/EC"). Considering the nature of this data, processing is forbidden unless the individual consents or if provided by national legislation.

This idea is echoed, in France, in its *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* modified by *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* du 6 août 2004 [3] (henceforth "Loi 78/17 modified in 2004"), in which article 8 details a series of exceptions to this prohibition.[4].

However, this notion is not found in all legislation. An analysis of European and Canadian documents demonstrates that generally health data is encompassed in notions and definitions of "personal information" or "personal data"[5]—in other words, all information that permits the direct or indirect identification of an individual.

1. Université de Montréal, Centre de recherche en droit public

 ISSN 1718-9314

Accordingly, "all information that allows the identification of an individual, whatever its range or degree of sensitivity, is therefore considered as personal data that receives equal protection under the law" (unofficial translation).[6]

In contrast, the Canadian *Personal Information Protection and Electronic Documents Act* (henceforth, "PIPEDA")[7], as well as provincial legislation in Alberta[8] Ontario,[9] Manitoba[10] and Saskatchewan[11] have adopted definitions of personal health data.

Does this situation mean that the processing—computerized or otherwise—of data related to health differs according to the understanding of the legislator? Our reading of the European and Canadian norms leads us to respond in the negative. We argue that by "processing," legislators refer to events that occur throughout the lifecycle of these data: in other words, from the collection of the data to its destruction irrespective of its personal or “health” nature.

This lack of a specific status for health data echoes fundamental principles set out since 1980, in the Organisation for Economic Co-operation and Development’s *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* [12] (henceforth "OECD Guidelines"), which the countries in the European Union, as well as Canada, follow. Does that mean that it is possible to communicate data electronically between Europe and Canada without taking special precautions? We would say no, because this question requires us to reconsider the place of the individual concerned: in other words, the patient, the participant in a research project, or their legal representatives. It is also necessary to rethink how the healthcare system is administered. Indeed, does the management framework for such transfers have to be done *in silo* or from a network paradigm?

To advance the latter option (as we will do and as other projects such as the *Système d’Information du Réseau Intégré de Laval* (*SI-RIL*) in Quebec and the personal medical file[13] or "carte Vitale" in France have done) involves revising the finality principle in order to ensure that the information used is of adequate quality for the intended purposes without creating the redundancy that results from repeated collections with privacy guarantees. It also requires us to rethink the personal data protection framework, considering that citizens interact with a variety of entities and thus require a climate of confidence and transparency. This is particularly so because "the more the required information is considered ‘sensitive,’ the more it is necessary to multiply the precautions in order to guarantee the necessary level of confidence" (unofficial translation).[14]

The understanding of crucial elements of the right of protection of health data necessitates framework in order to consider the challenges of computerized processing of health data.

I. Processing computerized health data: current framework

Normative instruments try to frame the processing of personal data for societies that increasingly function through networks. The observation of classical legal categories demonstrates that these texts indicate that "an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances," [15] or to ensure that the development of computerization does not " violate human identity, human rights, privacy, or individual or public liberties" (unofficial translation).[16] Though these texts are applicable within the scope they cover, the principles they prescribe are not necessarily applied to networks, that is, in interconnected environments in which information circulates in a multi-directional and non-hierarchical way.[17]

Consequently, how do we reconcile the need to exchange data between health professionals and/or researchers and the necessity of protecting individuals' reasonable expectations for privacy? How do we ensure that the legal standards protecting these expectations are binding for everyone in the network while making sure that the interpretation of these standards takes into account the proper functioning and efficiency of the network itself and allows people to have the best services?

Does **consent** still have to be the most important element in the computerization of health and social services and the growing development of multicentric, international research projects? Won't making consent the most important element reduce the flow of data? Isn't it likely to reduce the amount of data kept by the health system?

Though a significant part of the legal community remains attached to the supremacy of consent,[18] it appears poorly adapted to protect rights in the univers of networks. As practiced, consent seems more and more like a decoy since it seems to ensure individuals' control over their own data. The considerable number of exceptions as well as the way data circulate make consent naive at best, and at worst, an inadvisable instrument if we really do want to protect the privacy of participants. Faced with this situation, it is necessary to return to the essence of the relationship between an individual and a health professional and/or researcher and focus on the notion of confidence.

Instead of an act of consent frozen in time, a bond of confidence requires one of the parties in the relationship to depend on the other for the whole lifecycle of the personal data, and more specifically, of the health data. A true dialogue must be established between the transmitter and the recipient of the confidence, in order that the relationship remain transparent and to prevent mistrust from encroaching on confidence. This sentiment, necessary in a commercial activity, [19] must also prevail when we consider the computerized treatment of health data.

For that, it is important that the individual be informed about the purposes, which include the fact that the data could potentially be communicated, shared, or transferred electronically to another territory. There should also be transparency regarding security measures taken to ensure confidentiality and the quality of data throughout its lifecycle or even regarding the possibility of access to this data. The challenges of computerized processing of health data occur more at this level than at the level of research and the management of consent.

II. Computerized processing of health data: the issues

To allow the development of computerized processing of health data compatible with the respect for privacy (be it the interconnectedness of health establishments, access to personal medical files, the establishment of a smart card or in multi-centred or international research projects), it is necessary to address the challenges inherent to the issue. Without claiming to examine them all,[20] it could be useful to insist on the management of access rights and transborder flows of data.

Both European and Canadian standards require that processing occur with respect to individual rights such as confidentiality and right to access. These two precepts are antithetical only in appearance. Confidentiality does not imply that the health professional or researcher who collected an individual's health data cannot disclose it, transfer it, or share it with third parties. If we consider the multitude of exceptions contained in different documents aiming to protect the information that directly or indirectly identifies an individual,[21] these precepts imply that the exchange must be done only between authorized individuals and then only for the purposes delineated. In summary, sharing health data is a widespread practice, and it is commonly done for excellent reasons and with respect for individual privacy.

It is therefore advisable to make sure that confidentiality is never breached in the chain of exchanges; in other words, during the transmission or during the storage of data in a bank, for example. This is why confidentiality is linked with security measures.[22] In this context, the **management of rights of access** becomes a crucial tool of protection. The regulation of rights of access affects not only authorized individuals (generally speaking, health professionals and/or researchers in a research project) but also individuals (i.e. the patient, the research participant, or their legal representatives).

Relating to authorized individuals, it is necessary to determine whether access is absolute or limited to certain elements of the health file and/or the research file. Consequently, according to the choices of individuals, it is necessary to establish procedures allowing the identification of the person who wants to access a file and to determine his/her rights. This concept is included in two recommendations of the Council of Europe: one about the regulation of automated medical databanks and another about the protection of medical data (henceforth "Recommendation n°R(97)5").

Thus, in a project like the Canadian Molecular Cytogenetic Platform (henceforth "CMCP"),[23] it was decided that a doctor and/or researcher associated with the project could consult the files created by other members of CMCP. It is important to note that these files did not contain any identifying information about the individual, as stated in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*,[24] *Recommendation n°R(97)5*,[25] and the "*Loi 78/17 modifiée en 2004*".[26] Moreover, authorized access did not affect the information in the central databank, only the information which resulted from the research network(s) with which it was associated. There is therefore a control and a hierarchy of rights of access to the identifying information and the password.

Regarding the individuals involved, it is generally recognized that they have the right to access their own data.[27] However, taking into account the health repercussions of communicating this information, do we have to have a paternalistic approach to this right? Do patients or research participants directly exercise this right or do they have to ask their health professional and/or researcher to exercise this right for them? While some countries have long recognized the right of every individual to act directly, others have accepted this option only in the last few years and still work through an intermediary: for example, in France, where *Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé* adopted this approach in article L. 1111-7 of the public health act.[28]

Irrespective of whether these rights are exercised directly or not, the corollary is to allow the individual to ask for correction, even the suppression of all their data, with some exceptions: for example, aggregate data in a research project. This right—of access and of correction—must be carried out by the person responsible for the data processing.

This action by the individual also gives him/her the option of knowing whether his/her data has been tranferred across borders (**transborders flows)**. In effect, whether we consider European[29] (especially *Directive 95/46/EC*) or Canadian instruments, we see that they take into account the possibility of communication, sharing, and transferring individuals' health data to another province or another country, with the understanding that this would not change the rules about the protection of personal data in the original territory.

Consequently, the person responsible for the processing must ensure that the territory of destination for the data offers similar protection to that of the original territory. This precaution requires an extensive evaluation of the standards in use: for example, when a project entrusts data conservation to an operator outside the original nation or develops research that regroup different countries or provinces.

It is thus possible to state that the framework applied to all personal data, health data or otherwise, are similar in the countries of the European Union as in Canada, . As indicated earlier, these two entities have the same fundamental principles in terms of the protection of information that identifies, directly or indirectly, an individual. Consequently, it is possible to carry out computerized processing of health data between them after a preliminary analysis of the risks.

Conclusion

This analysis of the legal framework applied to the automated processing of health data indicates the necessity to reconsider the principles surrounding the protection of personal data in order to adapt them to the electronic environment. The changes induced by the move to information and communication technologies in health and social services must be accompanied by a redefinition, on the one hand, of the role of each party, making the distinction between authorized individuals and others affected by the data and, on the other hand, of the space in which personal data circulates.

[1] Strasbourg, January 28 1981, <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm> (page consulted January 15, 2006)

[2] Official Journal n° L 281 du 23/11/1995 p. 0031 – 0050, <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31995L0046&model=guichett&lg=en > (page consulted January 15, 2006).

[3] Official Journal of 7 August 2004, first article, <http://www.cnil.fr/index.php?id=301> (page consulted January 15, 2006).

[4] *Article 8 refers to this subject (the following is an unofficial translation):*
I. - It is prohibited to collect or process personal data which reveals, directly or indirectly, race or ethnicity; political, philosophical, or religious opinions; trade-union membership; or health or sexual information about an individual.
II. - Certain categories of data are not subjected to the prohibition of I :
1° treatments for which the individual consents, unless the law specifies that that the prohibition of I cannot be lifted through consent;
2° treatments necessary to protect human life, to which the individual cannot consent because of a legal incapacity or a physical impossibility; [...];
6° treatments necessary for preventative medicine, medical diagnosis, administration of care of services, or for the management of health services, and implemented by a health professional or someone else whose professional confidentiality is considered in article 226-13 of the penal code; [...];
8° treatments necessary to health research according to methods in chapter IX [Treatment of personal data in health research]
III. - If the personal data discussed in I are anonymized according to the law of the Commisssion national de l'informatique et des libertés, *this law could authorize [...] certain categories of processing according to the methods discussed in article 25 [authorization of the* Commission nationale de l'informatique et des libertés*]. The provisions in chapters IX and X [Processing of personal health data for the evaluation or analysis of healthcare practices and prevention activities] are not applicable.*
IV. - Similarly, computerized or non-computerized treatments justified by interest in the public good and authorized under conditions discussed in I of article 25 or in II of article 26 are not subject to the prohibition in I.

[5] Even if these concepts refer to information that allows direct or indirect identification of an individual, it is necessary to specify, on the one hand, that the term "personal data" is used by the members of the European Union, echoing *Directive 95/46/EC*. On the other hand, the term "personal information" reflects Canadian terminology as illustrated in the *Personal Information Protection and Electronic Documents Act* [2000, c.5] <http://www.iijcan.org/ca/sta/p-8.6> (page consulted January 15, 2006), *An Act respecting Access to documents held by public bodies and the Protection of Personal information*, R.S.Q. c.A-2.1 <http://www.iijcan.org/qc/laws/sta/a-2.1/index.html> (page consulted January 15, 2006) and *An act respecting Protection of personal information in the private sector*, R.S.Q. c. P-39.1 <http://www.iijcan.org/qc/laws/sta/p-39.1/index.html> (page consulted January 15, 2006).

[6] Richard E. LANGELIER, "Numérisation des dossiers de santé et protection des renseignements personnels, Impératifs techniques, intérêts économiques, considérations politiques et émergence de nouvelles normes," *Lex Electronica*, vol. 9, n°3, Summer 2004, p. 2, <http://www.lex-electronica.org/articles/v9-3/langelier.htm> (page consulted January 15, 2006). On the basis of this report, the author indicates that in Quebec, to bypass this situation, the legislature adopted numerous texts, of which An Act respecting health services and social services (L.R.Q., c. S-4.2) offers exceptions to the *Act respecting access to documents held by public bodies and the protection of personal information*. .

[7] Thus in PIPEDA, supra note 9, ""personal health information", with respect to an individual, whether living or deceased, means: 1) information concerning the physical or mental health of the individual; 2) information concerning any health service provided to the individual; 3) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; 4) information that is collected in the course of providing health services to the individual; or 5)information that is collected incidentally to the provision of health services to the individual.

[8] *Health Information Act*, R.S.A. 2000, c. H-5, <http://www.iijcan.org/ab/laws/sta/h-5/index.html> (page consulted January 15, 2006).

[9] *Personal Health Protection Information Act*, S.O. 2004, c. 3, Sch. A. <http://www.iijcan.org/on/laws/sta/2004c.3sch.a/index.html> (paged consulted January 15, 2006).

[10] *Personal Health Information Act*, C.C.S.M., c. P33.5, <http://www.canlii.org/mb/laws/sta/p-33.5/index.html> (paged consulted January 15, 2006).

[11] *Health Information Protection Act*, S.S. 1999, c. H-0.021, < http://www.iijcan.org/sk/laws/sta/h-0.021/index.html>.

[12] Paris, September 23, 1980.

[13] The notion of a personal medical file was introduced in French law by *Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie* "in order to support the coordination, the quality, and the continuity of healthcare, guarantee a high level of health, each recipient of health insurance has [...] a personal medical file made up of [...] information which allows follow-up on healthcare services" [unofficial translation]. Among the many commentaries on this file, see Olivier DUPUY, *La gestion des informations relatives au patient. Dossier médical et dossier médical personnel*, Bordeaux, Les Études Hospitalières, 2005.

[14] Pierre TRUDEL, "La vie privée dans les réseaux de soins au Québec," Lecture given through the International Institute of Research in Ethics and Biomedicine (IIREB), Faculty of Law, Université de Montréal, February 20, 2003.

[15] *Personal Information Protection and Electronic Documents Act*, L.C. 2000, ch. 5 article 3 (page consulted January 15, 2006)

[16] Loi 78/17 modifiée en 2004.

[17] For more on this subject, see Pierre TRUDEL, "État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement," presented during the National conference on "Technologies, vie privée et justice" [Technology, Privacy, and Justice], held in Toronto by the Canadian Institute for the Administraiton of Jusice (CIAJ), September 28 to 30, 2005 <http://www.chairelrwilson.ca/activites/icaj.html> (page consulted January 15, 2006); Pierre TRUDEL, "Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles," [2004] 110 *Revue française d'administration publique* 257-266.

[18] To demonstrate this, consult article L 161-36-1A of the *Code de la sécurité sociale*. This article, created by *Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie*, says that "two or more health professionals can, without opposition by an informed individual, exchange information..." [Unofficial translation]. <http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/decrets_application/2004-810.htm> (page consulted January 15, 2006). Also, see article 19 of *Loi sur les services de santé et les services sociaux*, modified by Bill 83 November 30, 2005, which confirms that "the file of a user is confidential and no one can access it without the consent of the user or of an individual who can consent in their place" [unofficial translation]. For an ethical analysis of consent, some possible sources are Christian BOUDREAU, Monica TREMBLAY, Bernard DUVAL et Nicole BOULIANNE, "Éthique du consentement à l'ère des réseaux d'information en matière de santé", in (2004) 6-2 *Éthique publique. Revue internationale d'éthique sociétale et gouvernementale* 54.

[19] For more on this subject, see Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, Montréal, Les Éditions Thémis, 2005.

[20] The challenges of computerization in health and social services require the revision of various principles inherent to the protection of personal data. Most notably, these include principles about the collection, the purposes, transparency, the quality of data, and responsibility. For more on this requirement, see Pierre TRUDEL, "État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement," presented during the national conference on "Technologies, vie privée et justice," held in Toronto by the Canadian Institute for the Administraiton of Jusice (CIAJ), September 28 to 30, 2005, http://www.chairelrwilson.ca/activites/icaj.html (page consulted January 15, 2006); Pierre TRUDEL, "Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles," [2004] 110 *Revue française d'administration publique* 257-266; Pierre TRUDEL, "La vie privée dans les réseaux de soins au Québec ," Talk given through the International Institute of Research in Ethics and Biomedicine (IIREB), Faculty of Law, Université de Montréal, February 20, 2003.

[21] Isabelle DUCLOS, "Qui, quand, pourquoi ? La confidentialité de votre dossier médical," (2005) 30-1 *Justice-Santé. La revue des usagers du réseau de la santé* 6.

[22] Liliane DUSSERRE, "La sécurité des échanges électroniques d'informations médicales nominatives entre médecins," Report adopted during a session of the *conseil national de l'Ordre des médecins*, April 2001, <http://www.web.ordre.medecin.fr/rapport/echangeselectroniques.pdf> (page consulted January 15, 2006), pp. 174-176.

[23] The authors of this article, with Mireille Lacroix and Rosario Duaso Calés of the Université de Montréal, participated in the development of this pancanadian, multi-centric project which aims to create a partnership that regroups 13 first-class research centres collaborating on an evaluation of a new technology for identifying chromosomal anomalies in children with serious mental disabilities of unknown cause. For more information, see <http://www.crdp.umontreal.ca/en/activites/biotechnologie/005.html> (page consulted January 15, 2006).

[24] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, 1998 (with modifications in 2000, 2002, and 2005), <http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm> (paged consulted January 15, 2006).

[25] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, 1998 (with modifications in 2000, 2002, and 2005), <http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm> (paged consulted January 15, 2006).

[26] Loi 78/17 modifiée en 2004.

[27] For more on the right to access information, see Herbert BURKERT, "Le droit d'accès en tant que droit de l'homme et l'éthique de la communication," in (2004) 6-2 *Éthique publique. Revue internationale d'éthique sociétale et gouvernementale* 42.

[28] In article L. 1111-7 of the public health code, it says that "all individuals have access to their health information held by health professionals and health establishments [...] they can access this information directly or through an intermediary, a doctor who they designate to obtain the information for them" [unofficial translation].

[29] For more on this subject, see Emmanuelle RIAL-SEBBAG, "Les échanges de données médicales en Europe et vers l'étranger," in Anne-Marie DUGUET, *Séminaire d'actualité de droit médical. Le secret professionnel. Aspects légaux et déontologiques. Comparaison avec l'étranger*, Bordeaux, Les Études Hospitalières, 2002; A.-M. DUGUET, J. BIGA, S. GUINART-DOUSSET, E. RIAL, "Échanges de données et de fichiers dans la recherche," Anne-Marie DUGUET, *Séminaire d'actualité de droit médical. Réseaux de soins, de santé et de recherche médicale. Aspects légaux et responsabilités. Bilan des expériences*, Bordeaux, Les Études Hospitalières, 2003.