Journal International de Bioéthique

Title: Juridical Protection of personal health information in Telemedicine in the MERCOSUR

Author: Jorge Nicolás Lafferriere

(Pontificia Universidad Católica Argentina)

Juridical Protection of personal health information in Telemedicine in the MERCOSUR

Author: Jorge Nicolás Lafferriere[1]

Abstract: This paper considers the legislation in MERCOSUR about the protection of personal information in Telemedicine. As Telemedicine is a new way of exercising medicine that involves new juridical challenges, we consider the topic within the general legal framework of the MERCOSUR. MERCOSUR is 20 years old and can be properly analyzed to verify how it has dealt with the topic of Telemedicine. Telemedicine involves different issues such as the problem of liability, the authorization to practice telemedicine, the protection of personal information, the system of payment and reimbursement, the informed consent and the relation between doctor and patient. We analyze only the protection of personal health information. We found out that there is no specific regulation of Telemedicine in the legal framework of practising medicine in MERCOSUR. We also analyzed the norms in Argentina and Brazil to draw some conclusions. Finally, we propose some guidelines for public policy.

Keywords: Telemedicine, Personal health information, informed consent, MERCOSUR.

Resumen: El artículo considera la normativa vigente en el ámbito del Mercosur en torno a la protección jurídica de los datos personales en Telemedicina. Atendiendo a que la Telemedicina es una nueva forma de ejercicio de la medicina que genera desafíos jurídicos, consideramos su encuadre jurídico general en el marco de las normas del MERCOSUR. Consideramos que el Mercosur resulta un buen encuadre de análisis, pues es un sistema de integración que tiene 20 años de antigüedad y que permite verificar cuánto se ha avanzado en la consideración jurídica de esta nueva realidad de salud. Dentro de los diversos tópicos jurídicos que involucra la telemedicina, tales como la cuestión de la responsabilidad de los profesionales, la habilitación profesional, la protección de los datos, los sistemas de pagos y reembolsos, el consentimiento informado y la relación médico-paciente, profundizamos lo relacionado con la protección de los datos personales. A tal fin, nuestro análisis señala que no hay normas específicas sobre la telemedicina en el sistema normativo del MERCOSUR. También se analiza la situación de Argentina y Brasil. Finalmente, en función de los resultados se consideran posibles lineamientos para políticas públicas en el tema.

Palabras clave: Telemedicina, Información sanitaria personal, consentimiento informado, MERCOSUR.

[1] Advocate, Universidad de Buenos Aires "UBA"; Doctor in Juridical Sciences, Pontificia Universidad Católica Argentina "UCA". Director of Applied Legal Research, Faculty of Law, Pontificia Universidad Católica Argentina, Professor Protitular of Principles of Private Law, UCA and UBA. Editor in Chief, Revista *Prudentia Iuris*. Director of the Center for Bioethics, Person and Family. Former Academic Secretary of Pontificia Universidad Católica Argentina. VicePresident of the International Academy for the Study of the Jurisprudence of the Family. This article is part of a research project between the Pontificia Universidad Católica Argentina and Grenoble Ecole de Management, under the direction of Nathalie Ferraud-Ciandet.

Résumé: Dans cet article on analyse la normative en vigueur dans le cadre du MERCOSUR vis-à-vis de la protection juridique des données personnelles en télémedicine. La télémedicine est une nouvelle forme d'exercice de la médicine qui pose des défis juridiques, et on considère en particulier son encadrement juridique général dans le contexte du MERCOSUR. On considère le MERCOSUR comme un point de départ intéressant pour notre analyse car il s'agit d'un système d'intégration avec plus de vingt ans depuis sa mise en œuvre, que nous permettra vérifier l'état des avances dans la considération juridique de cette nouvelle réalité dans le domaine de la santé. Parmi les nombreux sujets qui peuvent être abordées liées à la télémedicine, tels que la responsabilité civil des professionnels, l'habilitation pour l'exercice des professions, la protection des données personnelles, les systèmes de paiements et remboursements des services médicaux, le consentement informé, et la relation médecin-patient, on essayera de cibler celui de la protection des données personnelles. Avec cet objectif, notre analyse prend comme point de départ l'absence de normative spécifique sur la télémedicine dans le système normatif du MERCOSUR. La situation de l'Argentine et le Brésil est aussi considérée en particulière. Finalement, en fonction des résultats on présente des propositions de politiques publiques dans le domaine.

Mots clés: Télémédicine, Information sanitaire, consentement informé, MERCOSUR.

1. Telemedicine and its legal issues

Telemedicine is the practice of medicine at distance. The World Medical Association defines "Telehealth" as "the use of information and communications technology to deliver health and healthcare services and information over large and small distances"[13]. The eHealth resolution endorsed in Geneva in May 2005 by the World Health Assembly, the supreme decision-making body of the World Health Organization (WHO), affirms that eHealth "is the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research"[15],

Telemedicine implies new juridical challenges. Nathalie Ferraud-Ciandet considers that those issues are: on the one hand, the practice of telemedicine, which includes the licensing of physicians and the problem of payments and reimbursement; on the other hand, the liability issue, which includes the protection of personal data and the

consumer rights issue[3]. The Report presented by the Secretariat of the World Health Organization in 2005 recognizes that "eHealth issues pose new legal challenges. Many applications of eHealth are currently unregulated, unlike other aspects of the health systems. Legislation governing confidentiality, privacy, access, and liability is necessary with the transfer of information internally and externally"[10].

There are some important expectations over the social benefits of telemedicine. The report of the Secretariat of the World Health Organization says that eHealth "presents a unique opportunity for the development of public health. The strengthening of health systems through eHealth may contribute to the enjoyment of fundamental human rights by improving equity, solidarity, quality of life and quality of care"[10]. It also considers that "eHealth should have an impact on health systems by making health services more efficient and improving access to care, especially in remote areas, for people with disabilities and for the elderly. It should benefit health-care providers, professionals, and final users through higher quality of care and health promotion. It should also affect the cost of care by reducing redundancy and duplication of examinations and making possible economies of scale"[10]. We will not consider explicitly this issue in this paper, although we think that the legislation needs to protect personal data as a condition to achieve the best telemedicine.

In this paper, we will consider the problem of protecting personal information within the countries of the MERCOSUR. The importance of confidentiality and privacy in the use of personal data in telemedicine is acknowledged by the World Health Organization: "Ethical issues concern all countries in respect of confidentiality of information, dignity, and privacy"[10]. Also, the World Health Assembly urges "to mobilize multisectoral collaboration for determining evidence-based eHealth standards and norms, to evaluate eHealth activities, and to share the knowledge of cost-effective

models, thus ensuring quality, safety and ethical standards and respect for the principles of confidentiality of information, privacy, equity and equality"[15]. The importance of protecting confidentiality is recognized by a publication of the World Health Organization, when it states that "it is a good indicator of the extent to which wider legal issues in eHealth are being addressed at national and international levels"[12].

With this background, in this article we want to consider the situation of personal information within the telemedicine framework in the MERCOSUR, a regional Union between Argentina, Brazil, Paraguay and Uruguay[2].

2. Telemedicine and Health legislation within the MERCOSUR

"Mercado Común del Sur – MERCOSUR" (South Common Market) was founded in 1991 when Argentina, Brazil, Paraguay and Uruguay signed the Treaty of Asunción. The article 1 of the Treaty sets that the Common Market implies the commitment of the Member States to harmonize their legislations in the relevant areas to achieve the strengthening of the integration process. In 1997, the Member States signed the Protocol of Montevideo about the trade of services in the MERCOSUR.

In 1996, it was established the Working subGroup nro. 11 on "Health" (SGT nro. 11) by Resolution GMC Nº 151/96 [6]. The SGT N° 11 includes 3 working areas: Commission for Health Products; Commission on Epidemiological Surveillance and Health Control on Ports, Airports, Terminals and Frontiers; Commission on Health Services (Practicing and Health Technology). The subcommission on Health Technology pursues to harmonize the proceedings and standars for institutions and health centres, on levels of attention and complexitivity of the services.

[2] Venezuela signed a membership agreement on June 17 2006. Other countries have an associate member status: Bolivia, Chile, Colombia, Ecuador and Peru.

There are no specific regulations on telemedicine within the MERCOSUR. In our research, we found some generic Guidelines:

a) Resolution 18/05 of the Common Market Group (MERCOSUR/GMC/RES Nº 18/05) gives Guidelines for assessment of Methodologies in Health Technology. Resolution 18/05 defines Health Technologies as the "set of medicines, medical devices and procedure packs, used in health care, as well as organizational and supportive systems within which such care is provided also including the skills and knowledge required by Human Resources for Health Technology use, both in healthy and sick people". The Health Technology Assessment (HTA) involves research on the technical consequences (usually clinical), economic and social implications of the use of health technologies, including direct and indirect effects, intended and unintended, short and medium term.

b) Resolution 12/08 of the Common Market Group (MERCOSUR/GMC/RES Nº 12/08) regulates the application forms for this Health Technology Assessment.

c) Resolution 52/08 of the Common Market Group (MERCOSUR/GMC/RES. N° 52/08) establishes Guidelines for the reports on Health Technology Assessment.

d) Resolution 54/08 of the Common Market Group (MERCOSUR/GMC/RES Nº 54/08) establishes Guidelines for Promotion, Publicity and Advertising of Drugs in Mercosur.

e) Resolution 58/2001 of the Common Market Group (MERCOSUR/GMC/RES. nro. 58/2001) about Ethical medical principles of the MERCOSUR.

The conclusion is that there are some generic resolutions about health technology, but none of them contains specific regulations about telemedicine or the protection of personal health data.

3. Protection of personal information in Telemedicine in Argentina and Brazil

After considering the norms of the MERCOSUR and finding out that there are no specific regulations about telemedicine, we need to analyze the two major countries of Mercosur: Argentina and Brazil. Studying Argentina and Brazil will give us information about the existing legislation and it will help us to propose some guidelines for the MERCOSUR.

We will consider the issues related to telemedicine and the protection of personal health information, especially the regulation of electronic medical records, the ways in which personal health information is protected, privacy policy, criteria about disclosure of information, and criminal law about violating privacy and confidentiality.

3.1. Argentina

Argentina has some provisions about the protection of privacy in its Constitution, especially in Articles 18 and 19. Article 43, enacted in 1994, provides a right to *habeas data*: "Every person may file an action to obtain knowledge of the data about them and its purpose, whether contained in public or private registries or databases intended to provide information; and in the case of false data or discrimination, to suppress, rectify, make confidential, or update the data. The privacy of news information sources may not be affected".

The reform of the Constitution in 1994 gave some International Human Rights Treaties a constitutional status, including those that protect privacy and personal information. We must mention the American Convention on Human Rights (1969) that recognizes the right to privacy: "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against

such interference or attacks" (article 11). Also the International Convenant on Civil and Political Rights (1966) considers the right to privacy in its article 17.

In this constitutional framework, we should analyze the legislation that protects personal data:

a) Law 25.326 (B.O. 2-11-2000) of Protection of Personal Data. This law was passed in 2000 and regulates article 43 of the Constitution. In this law, health information is consider sensitive data (article 2). This law sets the need of previous informed consent to obtain, collect, store and use personal data (article 5). The information that has to be given to the person refers to the purpose of the data treatment, the information about the records, the consequences of giving up the information and other aspects (article 6). Article 7 establishes that no person must be compelled to provide sensitive data. Sensitive data can be collected and processed for compelling reasons of general interest authorized by law. It can also be treated with statistical or scientific purposes, always that their owners cannot be identified. Health data is regulated in article 8, setting that public and private health institutions and professionals involved in the health sciences can collect and process personal data relating to the physical or mental health of the patients, respecting the principle of confidentiality. Article 10 ratifies the duty of confidentiality. Article 11 regulates the transfer of personal data. It sets the need to request previous informed consent. But Article 11.2.e establishes that consent is not required in the case of transfer of personal health information if it is necessary for reasons of public health, emergency or epidemiological studies, preserving the identity of the owners of the data using appropriate dissociation mechanisms. Article 12 contains a specific regulation for international telemedicine. It regulates the international transfer and sets the general principle: it is prohibited to transfer any personal data to countries or international or supranational levels without adequate

protection. But article 12.2 sets the exceptions, so that the ban will not apply in the exchange of medical data, when required by the treatment of the diseased. But this article requires that in the exchange of medical data the patient should not be identified. This sets some problems for medical practice. This article contains a very important regulation about health records and telemedicine in its international aspect.

b) Law 25506 (2001) about digital certificates and signatures. It regulates the digital documents and the ways to certify the authenticity of a digital signature. It is a very important legislation for telemedicine since Decree 1089/2012, as it is required for electronic medical records.

c) Law 26.529 of Patient Rights in its relationship with the professionals and health institutions (2009), modified by Law 26742 (2012). Article 2 recognizes intimacy as a right of the patient and it orders that any health healthcare activity aimed at obtaining, sorting, using, managing, storing and transmitting information and clinical documentation of a patient should observe strict respect for human dignity and autonomy, and the protection of privacy and the confidentiality of sensitive data, without prejudice to the provisions contained in Law No. 25326 (article 2.c). Article 2 also recognizes a right to confidentiality (article 2.d). A key provision is article 13 about computerized medical record: "The content of the medical record, may be fashioned on magnetic media if there were arbitrated all means to ensure the preservation of its integrity, authenticity, fastness, durability and recoverability of data in the same time and form. To this end, it should be adopted with restricted access using identification keys, non-rewritable storage media, modifying control fields or any other suitable technique to ensure its integrity".

d) Decree 1089/2012 regulates the provisions of Law 26529. About confidentiality, this norm requires that everything that comes to the knowledge of health professionals

and their partners on the occasion or by reason of the exercise of medicine, and those who manipulate their clinical documentation, should not be made known without the patient's express permission, except cases that the law so determine, or in which there is an order from the justice to avoid a greater evil to public health. All these assumptions, shall be duly recorded in the medical record and, where appropriate, be made known to the patient. The duty of confidentiality extends to any person accessing clinical documentation, including those acting as insurers or funders of benefits. There is liability because of a breach on confidentiality not only of the professional but of the highest authority of the health care facility, and the social security institutions or other public or private body that accesses it (article 2.d, Decree 1089/2012). About the computerized medical record, the Decree 1089/2012 provides that the medical record must adapt to what is prescribed by Law 25.506, as supplemented and amended (article 13, Decree 1089/2012).

e) In the Penal Code, we should consider article 157 *bis*, which punishes the violation of confidentiality and security of personal information dabatases. This article was modified by Law 26.388 (B.O. 25/6/2008).

There are some resolutions taken by the Health Ministry setting the Health information integrated System (Sistema Integrado de Información Sanitaria –SISA-) and there are some federal offices to register health information (REFES – Registro Federal de Establecimientos de Salud, and RENIS – Registro Nacional de Investigaciones en Salud) [5].

3.2. Brazil

The 1988 Constitution of Brazil recognizes: "The privacy, private life, honor, and image of persons are inviolable, and the right to compensation for property or moral damages

resulting from the violation thereof is ensured" (article 5.X). It also protects telephone communications and data transfer as inviolable (article 5.XII) and it guarantees the access to information and the protection of the sources, when it is necessary for the professional practice. The Civil Code also protects private life as inviolable (article 21).

Although there is no specific law about telemedicine, the Health Ministry of Brazil has implemented the Telehealth Program (Programa Telessaúde)[3]. It is a national action program that wants to improve the quality of healthcare in the Unified Health System, integrating the technological resources. It began in 2007 and it includes knots of telemedicine in Universities in states of Amazonas, Ceará, Pernambuco, Goiás, Minas Gerais, Rio de Janeiro, São Paulo, Santa Catarina and Rio Grande do Sul. The Telehealth Program includes the following practices: I) Teleconsulting, which includes synchronous-teleconsulting or asynchronous-teleconsulting; II) Telediagnosis; III) Formative Second Opinion; IV) Teleeducation[4]. The structure of the Telehealth network includes: a) The National Coordination exercised by the Ministry of Health through the Department of Labor and Management in Health Education (SGTES / MS) and the Department of Health Care (SAS / MS); b) State Coordinations, exercised by the Health Department of each State or the Federal District; c) State Management Committee; d) Scientific-Technical Center for Telehealth, and e) the City Manager of Health. The Ministry of Health created in 2010 the Permanent Commission on Telehealth[5]. In 2012, the Ministry of Health published the "Telehealth Manual for Primary Care"[6] where the different services are explained.

Concerning the issue of protection of personal health information, we must take into account:

---

[3] http://www.telessaudebrasil.org.br/

[4] Ministério da Saúde, Gabinete do Ministro, Portaria Nº 2.546, de 27 de outubro de 2011.

[5] Ministério da Saúde, Gabinete do Ministro, Portaria Nº 452, 4 de março de 2010.

[6] "Manual De Telessaúde Para Atenção Básica / Atenção Primária À Saúde", Ministério da Saúde. Universidade Federal do Rio Grande do Sul, 2012.

a) Law 8078 (11/09/1990) regulates the protection of consumers. This Law sets standards for protection of consumers for public order and social interest. It regulates article 5.XXXII of the Federal Constitution. There is a controversy about the practice of medicine. While some of the authors consider that the relation between the physician and the patient is a consumer relation, others disagree on the basis of the Medical Ethical Code [7]. This Code regulates the access to records and personal data stored in databases (article 43).

b) Law No. 9507 (12 November 1997) regulates the right of access to information and procedural discipline rite of habeas data.

c) The Resolution 4279 of the Ministry of Health (30-12-2010), that sets the guidelines for the organization of the Healthcare Network within the Unified Health System.

d) The Resolution 2073 of the Ministry of Health (31-8-2011) regulates the standards for interoperability and health information for health systems.

e) The Resolution 1643/2002 of the Federal Medical Council (07-08-2002, Conselho Federal de Medicina, CFM)[7], which defines Telemedicine as the practice of medicine through interactive methods of communication of data, with the purpose of care, education and research in health (art. 1). Article 2 sets the duty of the services of Telemedicine to fullfill the requirements of confidentiality and privacy and professional secrecy in the handling of health information. The juridical persons that provide telemedicine should be part of the registry of telemedicine in the Regional Council of Medicine of each state.

[7] Ronaldo Behrens gave me the information about the CFM regulations in Brazil during his presentation in the Seminar about Telemedicine, Ethics and Law held in Pontificia Universidad Católica Argentina on June 26, 2013.

f) The Resolution 1638/2002 of the Federal Medical Council (9-8-2002) which defines the medical records (prontuário médico) and sets the requirements that health centres should accomplish.

g) The Resolution 1821/2007 of the Federal Medical Council (23-11-2007 approves the guidelines of digitalization and use of informatic systems to gather and use health documents. Article 2 requires that digital records should accomplish some conditions, including security levels ("Nível de garantia de segurança 2 NGS2). It requires digital signature (art. 5).

h) In the Penal Code, article 153 punishes the disclosure of private or confidential information without cause. Article 154 punishes the breach of confidentiality.

4. Conclusions and public policy proposals

4.1. Some conclusions

After this analysis, we can come to some conclusions about the legal protection of personal data in telemedicine in the Mercosur:

a) Mercosur: There are no specific regulations about telemedicine, or about the protection of personal data in health systems. There are some resolutions about Health Technology Assessment but none of them has direct relation with the protection of personal health information.

b) Argentina: There is no specific regulation about telemedicine and there is not a specific program within the Ministry of Health. However, the Constitution explicitly protects personal information and there are strong national regulations protecting personal health information, which is considered sensitive data. Law 25326 contains specific norms about transferring personal health information to another country (article 12). Law 25506 regulates secured digital signature and gives a very important

framework for electronic health records, as it is set by Decree 1089/2012 and Law 25629. There are also criminal law provisions to punish the violation of privacy and confidentiality.

c) Brazil: Guidelines for Telemedicine are set by the Federal Medical Council and those guidelines include the duty of privacy and confidentiality. There is a National Program on Telemedicine under the Ministry of Health. There is a growing experience in the coordination of telemedicine efforts. However, there is no specific legislation about the protection of personal health information, although it must be understand that it is included in the constitutional protection of the rigth to privacy. There is a law regulating the *habeas data*.

The MERCOSUR situation appears to be very similar to the results of the second global survey on eHealth conducted by the Global Observatory for eHealth (GOe), set out to investigate "the extent to which the legal frameworks in the Member States of the World Health Organization (WHO) address the need to protect patient privacy in electronic health records (EHRs) as health care systems move towards leveraging the power of EHRs to deliver safer, more efficient, and more accessible health care" [12]. Survey results show that a generally sound base of generic privacy protection exists: "some 70% of the 113 responding countries reported having legislation providing a basic right to privacy, and the remaining 30% anticipate that such legislation would be adopted by 2015. When reviewing the existence of legislation specifically protecting the privacy of the EHR these values are reversed, however: only 30% globally reported having such legislation in place. Further analysis of the responses on the use of legislation to ensure privacy in sharing EHRs for treatment or research purposes reveals that very few countries have established comprehensive legal frameworks on EHRs

(e.g. only 10% of countries reported having legislation which covers cross-border EHR sharing)" [12].

This survey makes clear however that "while comprehensive human rights laws, such as constitutions or civil rights laws, often address some element of informational privacy, only a few countries have specific sectoral legislation addressing medical privacy; even fewer have legislation which specifically covers privacy and other patients' rights in EHRs. The eHealth survey found equally that although a reasonably high level of comprehensive laws addressing certain aspects of privacy that apply to EHRs existed, only a few countries have laws which specifically address the issue of medical records privacy, and even fewer have laws focused on privacy of EHRs" [12].

Within the Pan American Health Organization, an important study talks about a "patchwork regulation" and acknowledges that "except for the standardization effort of the European Community and the OECD countries, each country's legislative, executive and judicial systems are addressing electronic health data regulation in differing ways. Complicating the present patchwork system of laws is the lack of uniformity in the area of electronic health information" [9].

New questions arise after this study about the legislative approach to personal health information protection within the MERCOSUR. Should there be a specific regulation of telemedicine within the Mercosur? Are national regulations enough to prevent problems? Is it a problem related to development conditions? Is it because telemedicine is not a priority in the area, except from Brazil? [1].

We can not answer to all these questions now, but we can make some recommendations to improve the protection of personal health information in the MERCOSUR.

4.2. Public policy proposals

Given these conclusions, we finish this article suggesting some public policy questions and proposals:

a) It is important to start negotiations towards protecting personal information in telemedicine within the MERCOSUR. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 could give some guidance on this matter. This Directive "aims to establish rules for facilitating access to safe and high-quality cross-border healthcare in the Union and to ensure patient mobility in accordance with the principles established by the Court of Justice and to promote cooperation on healthcare between Member States, whilst fully respecting the responsibilities of the Member States for the definition of social security benefits relating to health and for the organisation and delivery of healthcare and medical care and social security benefits, in particular for sickness". In particular, Directive 2011/24/EU recognizes that "the right to the protection of personal data is a fundamental right recognised by Article 8 of the Charter of Fundamental Rights of the European Union. Ensuring continuity of cross-border healthcare depends on transfer of personal data concerning patients' health. These personal data should be able to flow from one Member State to another, but at the same time the fundamental rights of the individuals should be safeguarded. 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 establishes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Those provisions should also apply in the context of cross-border healthcare covered by this Directive".

b) A future regulation within the MERCOSUR about telemedicine should recognize the protection of the fundamental right to privacy with respect to the processing of personal data in conformity with national measures implementing provisions on the protection of personal data[8]. It should be pointed out that on January 25, 2012, the European Commission released a proposed General Data Protection Legislation ("Proposed Regulation") for comprehensive reform of existing European Union ("EU") data protection rules. The current governing law is the 1995 EU Data Protection Directive, which has been implemented differently by the 27 member states, so the proposed Regulation aims to harmonize data protection rules throughout the EU[9].

c) A future regulation should distinct between the Member State of Affiliation and the Member State of Treatment[10].

d) The regulation should recognize the right of patients who seek to receive or do receive cross-border healthcare to have remote access to or have at least a copy of their medical records, in conformity with, and subject to, national measures implementing provisions on the protection of personal data[11].

e) There are important recommendations made by the Standing Committee of European Doctors about Telemedicine [11], including the guidelines for e-mail correspondence in patient care. Also, they recommend that the transfer of personal data outside the European Union should be forbidden unless confidential processing of data has been ascertained in the destination. This recommendation should be taken into account in MERCOSUR.

f) Encryption is also an important issue to protect confidentiality. As the World Medical Association recommends: "Data obtained during a telemedical consultation must be

[8] cf. Directive 2011/24/EU Article 4.2.e.
[9] http://hstlj.org/european-commission-proposed-data-protection-law/ (22-3-2013). Also see: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (22-3-2013)
[10] cf. Directive 2011/24/EU Chapter II, articles 4 and 5.
[11] cf. Directive 2011/24/EU Article 5.d.

secured through encryption and other security precautions must be taken to prevent access by unauthorized persons"[14].

g) It is important to protect personal health and genetic information as sensitive data and impose the safeguards that this kind of information requires[8].

h) The previous and informed consent of the patient is essential in the use of telemedicine.

These are some provisions that could be included in a regulation of telemedicine within the MERCOSUR. We have not included all the possible issues in discussion and we tried to focus on the problem of the protection of personal health information[12]. We hope a regulation about telemedicine is achieved in the next years in MERCOSUR as a way to improve healthcare in the region.

Bibliography:

[1] De Ortúzar, M.G., *To Telemedicine in MERCOSUR A Comparative Ethical Review of the Laws of Brazil and Argentina*, Revista eSalud.com, 2012, Vol. 8, Issue 30, pp.1-17.

[2] Ferraud-Ciandet N., *Droit de la télesanté et de la télémédecine. À jour du décret du 19 octobre 2010 su la télemédicine*, Paris, Editions Heures de France, 2011, 159 p.

[3] Ferraud-Ciandet N., *L'Union européene et le télésanté*, Revue Trimestrielle de droit européen, Juillet / Septembre 2010, nro. 3, pp. 537-561.

[4] Ferraud-Ciandet N., *Sécurité et confidentialité des données de santé dans l'Union européenne. Le cadre legal applicable aux dossiers médicaux électroniques nationaux*, Revue Européenne de Droit de la Consommation, Vol. 3, pp. 417-424.

[12] For a broader analysis, see [4, 2].

[5] Ferraud-Ciandet N., *Ética y Derecho en telemedicina argentina*, Revista El Derecho, 13228, pp. 1-3.

[6] Fraga D., *Presentación de la Secretaría Administrativa del MERCOSUR (SAM) en la Reunión de "Importancia de la Información Jurídica en Internet: Explorando las Interrelaciones Nacionales e Internacionales*, Uruguay, 2001, (cited 2012 May 19). Available from: http://crics5.bvsalud.org/E/grupos/grupo1/Fraga.pdf

[7] Gozzo D., *Transparência, Informaçäo E A Relaçao Mèdico-Paciente.* In: Gozzo D., editor, *Informaçao e Direitos Fundamentais. A eficacia horizontal das normas constitucionais*, Sâo Paulo, Editora Saraiva, 2012, pp. 75-90.

[8] Lateef F., *The practice of Telemedicine: Medico-legal and Ethical Issues*, Ethics & Medicine, Spring 2011, Vol. 27:1, pp. 17-24.

[9] Rodrigues R.J., Wilson P., Schanz S.J., *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information. An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-Identifiable Health Databases*, Pan American Health Organization, Washington DC, 2001.

[10] Secretariat of the World Health Organization, *Report on Ehealth*, A58/21, 7 April 2005, (Cited 2012 May 19). Available from: http://www.ctc-health.org.cn/file/20090219046.pdf.

[11] Standing Committee of European Doctors (CPME), *CPME guidelines for Telemedicine,* 2002 (cited 2012 May 19), http://cpme.dyndns.org:591/database/Telemedecine_2002.pdf.

Traducción castellana: No

Comprobado el 16 de mayo de 2002

[12] World Health Organization, *Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. (Global Observatory for eHealth Series, v. 5)*, Geneva: World Health Organization; 2012 (cited 2012 May 19). Available from: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

[13] World Medical Association, *Statement on Guiding Principles for the Use of Telehealth for the Provision of Health Care*, *Adopted by the 60th WMA General Assembly, New Delhi, India, October 2009*, (cited 2012 May 19). Available from: http://www.wma.net/en/30publications/10policies/t5/index.html

[14] World Medical Association, *WMA Statement on Accountability, Responsibilities and Ethical Guidelines in the Practice of Telemedicine*, *Adopted by the 58th WMA General Assembly, Copenhagen, Denmark,* October 2007 (Cited 2012 May 19). Available from: http://www.wma.net/en/30publications/10policies/20archives/a7/

[15] World Health Assembly, *Resolution on eHealth*, Geneva, May 2005, (Cited 2012 May 19). Available from: http://extranet.who.int/iris/bitstream/10665/20378/1/WHA58_28-en.pdf