SHS Web of Conferences **2**, 00013 (2012)
DOI: 10.1051/shsconf/20120200013

Data protection in telemedicine

A. Gusarova

Rīga Stradiņš University, Latvia

Abstract. Telemedicine – is the use of information and communication technologies in the situation when health care professional and the patient are not in the same location. That means that health care services are provided from the distance. The telemedicine services include transmission of information about patients' health through text, sound, images and other data forms for the prevention, diagnosis treatment and follow-up of the patient. The use of telemedicine services contributes to health improvement and its application should be considered favourably. However, it is necessary to be aware that the use of different telemedicine solutions includes processing of patient's data. Thus, this issue should be considered from the perspective of data protection. Despite the fact that the use of telemedicine services will positively makes changes in relationship between health care professional and patient that should not negatively affect persons' rights to data protection. The person who receives health care services is entitled to expect that health care service will be provided with the respect to human rights.

Key words: *telemedicine, health care, e-health, data protection*

Information technologies have become a part of our everyday life. Many processes of our business and private life now are based on the use of information technologies due to the advantages information technologies gives. The health sector is not the exception – in the health sector as well it is necessary to introduce a new kind of creation, storage and circulation of information that would serve needs of every person who is involved in health care (needs of medical practitioner/hospital/other health care professionals/health care recipient – patient).

Telemedicine is new kind of provision of health related services which improve quality and accessibility of health care by integrating information and communication technologies in health sector. Fundamental activities in this field dates back to the seventies and especially to the eighties of the 20th century, when the personal computer revolution took place (Ferrer-Roca, Sosa-Iudicissa, 2002).

There is no generally accepted definition of telemedicine. But, according to the one of the most widely used definitions – telemedicine is the use of information and communication technologies to transfer medical information for the delivery of clinical and educational services (Norris, 2001). Telemedicine by its nature is the use of information and communication technologies in the situation when health care professional and the patient are not in the same location, what means that health care services are provided from the distance. The following conclusions can be made looking at the literal meaning of the word "telemedicine": this term is a combination of two words: "*tele*" which derives from the Greek meaning "at a distance" and "medicine" which derives from the Latin "*mederi*" meaning "healing" (Lievens, Jordanova, 2007). So, telemedicine is a different way of delivering health care.

Competence of EU and Latvia regarding telemedicine

Both the European Union (further EU) and national level in Latvia as a political objective have been determined introducing information and communication technologies in health sector (White Paper "Together for Health: A Strategic Approach for the EU 2008–2013"; Regulation of the Cabinet of Ministers of the Republic of Latvia No 560 "Guidelines for e-Health in Latvia"). Allocation of

responsibilities for public health policy between the EU and Latvia as Member State of EU is as follows: public health area does not fall within exclusive competencies of EU, and EU shall take action, in accordance with the principle of subsidiarity, only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States and can therefore, by reason of scale or effects of the proposed action, be better achieved by the EU (The Treaty on the Functioning of the European Union). That means that EU action serves as a complementary action to Latvia's action. (Commission communication "Telemedicine for the benefit of patients, healthcare systems and society"; Directive 2011/24/EU).

The legal framework of telemedicine consists of EU law and national laws of Latvia. Legal framework of telemedicine at the EU level relatively can be divided into the following area (due to principle of subsidiarity specific provisions of health services are governed by existing secondary legislation): the cross-border provision of services (telemedicine should be viewed both from the perspective of information society and health service), data protection and privacy and liability. Directives related to data protection in telemedicine context are: Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (further Directive 95/46/EC) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. The second one in data protection context widely reflects to requirements included in Directive 95/46/EC. That means that Latvia in general keeps political and regulatory competence regarding health care, i.e. telemedicine. However, legal framework at the national level in Latvia consists of laws where duties regarding data protection are specified in very general manner and only in specific circumstances provides clear guidance on this matter (for example, Law On the Rights of Patients, Medical Treatment Law, etc.). Due to the fact that there is no specific regulation regarding provision of telemedicine services, regarding these services are applicable general data processing principles contained in Personal Data Protection Law (further PDPL), which is an instrument of implementation into Latvian national legislation of Directive 94/46/EC.

Such a conclusion is justified because the fact that telemedicine is a service delivered by electronic means does not constitute a reason for treating telemedicine as a special type of health services. The following conclusions are made by the European Court of Justice (Case C-385/99 *Müller and Van Reit* [2003] ECR I-4509; Case C-157/99 *Smits and Peerbooms* [2001] ECR I-5473; Case C-372/04 Watts [2006] ECR I-4352; Case C-159/90 *Society for the Protection of Unborn Children Ireland* [1991] ECR I-4685; Joined Cases 286/82 and 26/83 *Luisi and Carbone* [1984] ECR 377) deciding on the patient's right to cross-border health care. In accordance with the mentioned above, can be concluded that to telemedicine as a new kind of provision of medicine services (medicine at distance) applicable are the same requirements as plain medicine: use of qualified personnel, an unambiguous legal framework defining the rights and obligations of patient and health care provider, and well-defined quality standards (Ferrer-Roca, Sosa-Iudicissa, 2002).

The concept of personal data in the context of telemedicine

In accordance with the PDPL (Article 2 (3)) and Directive 95/46/EC (8, Article 2 (a)) personal data is any information relating to an identified or identifiable natural person (data subject) and an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Due to the mentioned above, information related to persons health as well shall be considered as personal data.

And, processing of personal data shall mean 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 (it is difficult

to envisage any activity involving data which does not amount to processing) (Article 2 (4) of PDPL and Article 2 (b) of Directive 95/46/EC).

Considering the format or the medium on which that information is contained, the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. This is a logical consequence of covering automatic processing of personal data within its scope. In particular, sound and image data qualify as personal data from this point of view, insofar as they may represent information on an individual. This is further clarified by Recital 14 of Directive 95/46/EC which states that given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data (Opinion No 4/2007 on the concept of personal data).

Telemedicine encompasses a wide variety of services and those most often mentioned in peer-reviews are teleradiologys, telepathology, teledermatology, teleconsultation, telemonitoring, telesurgery and teleophthalmology (Commission communication "Telemedicine for the benefit of patients, healthcare systems and society"). Due to the fact that providing the above mentioned services involves personal data because these services include transmission of information about patients' health through text, sound, images and other data forms for the prevention, diagnosis treatment and follow-up of the patient, this issue should be considered from the perspective of data protection.

General personal data protection principles

Assessing the evolution of the legal framework for privacy in the historical context, several privacy protection instruments have been adopted already in 1970's to the 1980's, due to the rapid technological progress of information and technologies worldwide, what created new risks to privacy (Korff, 2005). Although legal protection of personal data have been clearly defined relatively recently, opinion that processing of information containing personal data on health should be strictly limited, has developed a long time ago, i.e. long before protection have been determined to other privacy-related information. "The medical profession's ethical requirement of confidentiality was first set out in the "Hippocratic Oath" and subsequently affirmed by the World Medical Association's Declaration of Geneva (1948)" (Working document No 131 "Working Document on the processing of personal data relating to health in electronic health records (EHR)"). Hippocratic Oath was formulated around the 5th century BC (it is assumed to believe that the first time that was formulated by the father of Western medicine – Hippocrates, and the oath is still well known worldwide and is being used), and that states that whatever medical professional see or hear in the lives of his patients, whether it is connected with his professional practice or not, medical professional ought not to be spoken of outside, and will kept in secret, as considering all such things as private (Dossetor, 2005). As evidence that person's right to protection of information related to health or closely related to that has a fundamental importance acknowledges the fact that unwritten ethical principles of Hippocratic Oath now have been formulated in legal framework. As well, requirements for the protection of such information have become stricter and detailed compared to the Hippocratic Oath.

Personal data protection rights in Latvia deriving from an individual's right to privacy enshrined in Article 96 of Constitution of the Republic of Latvia, as well obligation arising from other to the Republic of Latvia binding human rights instruments: Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Human Rights Convention, Article 17 of the International Covenant on Civil and Political Rights. Besides, by recognizing the current and future development of the information and communication technologies and its impact on person's privacy, the person's rights to data protection now are determined as independent legal right in the European Union Charter of Fundamental Rights.

Thus, the data protection rights are ranked among other human rights as independent rights with clear legal protection.

Person's right to data protection by its nature includes persons rights to determine what personal information person wants to make available to other, as well rights to know: who, what, for what reason collecting and storing information regardless of whether it is in favor of person or not (Vilbergs, Krasts, 2002). Alan Westin (researcher on privacy issues) has defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1968).

However, data protection rights are not absolute rights, because these rights are subject to reasonable restrictions in certain circumstances for reasons of substantial public interest. Certainly, assessing whether a restriction on rights is justified, should be considered the following: 1) the restriction should be prescribed by law, 2) it should be directed to a legitimate objective and 3) it should be necessary in a democratic society (the restriction should be socially necessary and proportionate) (Judgment of the Department of Administrative Cases of the Supreme Court Senate of the Republic of Latvia, case No.SKA-347/2010, clause 8). It also complies with regulation set in Article 116 of the Constitution, which states that a person's right under the Article 96, 97, 98, 100, 102, 103, 106 and 108 of the Constitution of the Republic of Latvia may be subject to restrictions in circumstances provided for by law in order to protect the rights of other people, the democratic structure of the State, and public safety, welfare and morals.

Besides, data concerning health of the person are identified as a special category of data (sensitive data) (Article 8 (1) of Directive 95/46/EC; Article 2 (clause 8) of PDPL), and conditions for processing of such data are more strict, i.e, circumstances when such data processing is permitted have been defined as an exception from general prohibition of processing of such data (special provisions have been strictly determined) (Article 8 (2), 8 (3), 8 (4) of Directive 95/46/EC; Article 11 of PDPL). It should be noted that regardless of whether that information directly provide information about health of the person or indirectly, what is the amount of information (including information which is inherently non-health data, but closely related to it) to a person's life period of the concerns: the individual's past, present or future physical or mental health, how it is processed (oral, written, electronic) and who perform processing (health care provider, public health authority, employer, insurer, educational institution, etc.), data protection requirements are applicable, in particular requirements concerning processing of special categories of data.

Requirements which have been defined as universal data protection principles can be divided as follows:

1) requirements regarding legitimacy of processing of personal data (Article 7 and 8 of Directive 95/46/EC; Article 7, 10 (clause 1), 11 of the PDPL);
2) requirements regarding the purpose for the processing of personal data (Article 6 (1) (b) of Directive 95/46/EC; Article 10 (clause 2) of PDPL);
3) requirements regarding amount of personal data (Article 6 (1) (c) of Directive 95/46/EC; Article 10 (clause 2) of PDPL);
4) requirements regarding data quality (Article 6 (1)(d) of Directive 95/46/EC; Article 10 (clause 3 and 4) of PDPL);
5) requirements regarding ensuring rights of data subjects in accordance with the relevant requirements for governing data protection (right of access, rectification right, blocking right, erasure right, right to object, right of notification to third parties, rights related to automated individual decisions, rights to be informed about data processing, etc.) (Article 10, 11, 12, 14 of Directive 95/46/EC; Article 8, 9, 15, 16, 17, 18, 19 and 20 of PDPL);
6) requirements regarding data security (Article 17 of Directive 95/46/EC; Article 25 of PDPL);
7) requirements regarding duration of processing of personal data (Article 6 (e) of Directive 95/46/EC; Article 10 (clause 3) of PDPL);

8) requirements regarding personal data transfer outside European Economic Area (Article 25 of Directive 95/46/EC; Article 28 of PDPL).

In the context of provision of telemedicine services the first principle is the most important due to the fact that existence of the legal base for data processing allows processing of personal data as such and based on this legal framework is established boundaries of processing personal data.

Legal base for processing of personal data in telemedicine

The basic condition for processing of personal data is existence of legal base for such processing. In case of traditional health care provision it is assumed that processing of personal data of patient is carried out on the bases of the following principles (necessary for legitimising processing):

- the data subject has given his explicit consent to the processing of those data (Article 8 (2) (a) of Directive 95/46/EC; Article 11 (clause 1 of PDPL);
- person' s data processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent (Article 8 (2) (c) of Directive 95/46/EC; Article 11 (clause 3) of PDPL);
- processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (Article 8 (3) of Directive 95/46/EC; Article 11 (clause5) of PDPL).

Regarding telemedicine is reasonable to assume that generally would be applicable the first principle, and in exceptional cases – the second. The third principle would not be applicable what is associated with individuals' rights to autonomous self-determination of health care context and specific nature of telemedicine.

In accordance with Article 6 (4) of Law on the Rights of Patients, a patient has the right to refuse medical treatment prior to the commencement thereof, from any method used in the medical treatment, without declining from the medical treatment at large, or to refuse medical treatment during it. That fully connected to patient's rights to autonomy – a patient's right to self-determination with regard to healthcare. As well, the patient's rights to self-determination also means to undertake the need for informed consent and correlatively a health care professional's duty to inform adequately to the patient previously to give his or her consent (Romeo-Casabona, 2008).

So, regarding the use of telemedicine services can be assumed that patient has a right to refuse or consent to telemedicine services, i.e., health care provider must obtain a patient's consent before provision of telemedicine service. It is clear that a patient may be willing to receive treatment but only by conventional means and not by telemedicine, for example, patient may refuse use of telemedicine services on moral or religious grounds.

On the bases of the mentioned above, it can be assumed that realization of rights to information has direct effect to the realization of rights to self-determination with regard to health care. And, due to the specific nature of telemedicine services, it is necessary that patient gives his consent for provision of telemedicine services. Criterion on which depends the validity of the consent are the following (defined in Article 2 (h) of the Directive 95/46/EC; Article 2 (clause2) of PDPL):

- consent must be freely given;
- consent must be given to clearly specified purpose;
- consent must be based on sufficient information.

The criteria "*freely given*" means that the patient's decision should not affect him in any other way and the consent form must be sufficiently convincing. As well, that means that health care provider should give the opportunity to the patient to refuse or limit their consent. The criteria "*for clearly specified purpose*" means that the purpose should be stated very clear and cannot be general, i.e., should be clear reference to the use of telemedicine services. The criteria "*on the bases of sufficient information*" means that patient have been informed (including, answers of the patient's questions and concerns) of the options available to them. The duty to give information should be realized in a way that guarantees that the patient has clear understanding of the nature of telemedicine service due to the fact that the way this service is guaranteed is more complex than it could seem at first sight. Information must be sufficient and respecting the level of understanding of the patient. As well, it should be noted that telemedicine, first of all, is great challenge for healthcare professionals due to the fact that it is a different kind of provision of health care services. Health care professionals have thus been forced to acquire more in-depth and more specialized knowledge and skills to enable them to practice properly and correctly and this in turns has had further implications: an increase in the obligations which a physician has to fulfill in the course of his or her work. These range from general obligation – the need for better training and higher qualifications – to more specific ones entailed in his or her relationship with each particular patient, such as a duty to inform and the duty to secrecy (Romeo-Casabona, 2008). Good knowledge of the nature of telemedicine service is necessary due to the fact that exactly health care provider is a person who use telemedicine services and ensure that health care provision is in compliance with the patient rights prescribed in legislation.

In addition, taking into account that there is no strict legal framework regarding form of consent, it is necessary to be aware that the evidence of patient consent existence does remain on the health care provider. It is necessary to consider that consent in written usually will be more effective proof of consent existence for health care provider. And, even if consent have been in written, that always should be accompanied by a verbal explanation of how the system will work, to ensure that the patient has reasonable information on which to base a valid consent.

References

[1] Dossetor, J.B. (2005) Beyond the Hippocratic Oath: A Memoire on the Rise of Modern Medical Eethics. Canada: The University of Alberta Press, 301 p.

[2] Ferrer-Roca, O. and Sosa-Iudicissa, M. (eds) (2002) Handbook of Telemedicine (Third printing). The Netherlands: IOS Press, 297 p.

[3] Korff, D. (2005) Data Protection Laws in the European Union. U.S.A: Federation of European Direct and Interactive Marketing and The Direct Marketing Association, 323 p.

[4] Norris, A.C. (2001) Essentials of Telemedicine and Telecare. England: John Wiley & Sons, Ltd, 183 p.

[5] Vilbergs, H.J., Krasts, V. (2002) Salīdzinošās administratīvās tiesības: lietas un risinājumi [Comparative Administrative Law: Cases and solutions]. Rīga: N.I.M.S., SIA, 441 p.

[6] Westin, A. (1968) Privacy and freedom (Fifth ed.). New York: Atheneum, 487 p.

[7] Lievens, F., Jordanova, M. (2007) Telemedicine and Medical Informatics: The Global Approach. World Academy of Science, Engineering and Technology. Issue 0031: 2007, (p. 258-262). http://www.waset.org/journals/waset/v31/v31-45.pdf.

[8] Romeo-Casabona, C.M. (2008) The legal approach to medical liability. Negligence and breach of patient's autonomy. In European Conference on "*The ever-growing challenge of medical liability: national and European responses",* 2-3 June 2008 (p. 109-119). Strasbourg: the Council of Europe, Directorate General of Human Rights and Legal Affairs.

[9] The Universal Declaration of Human Rights. General Assembly of the United Nations, 10.12.1948. http://www.un.org/en/documents/udhr/

[10] 15.02.1922. Law "Constitution of the Republic of Latvia"//with amendments announced till 29.04.2009. Official Newpaper of the Republic of Latvia *Latvijas Vēstnesis* No 43, 01.07.1993.
[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union* L 281.
[12] 23.11.1995. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
[13] 04.06.1997 Law "On the 04.11.1950 Convention for the Protection of Human Rights and Fundamental Freedoms" and its Protocols 1, 2, 4, 7 and 11. Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 143/144, 13.06.1997.
[14] 23.03.2000 Law "Personal Data Protection Law"// with amendments announced till 19.05.2010. Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 123/124, 06.04.2000.
[15] 16.12.1966. International document "International Covenant on Civil and Political Rights". Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 61, 23.04.2003.
[16] 17.08.2005 Regulation of the Cabinet of Ministers of the Republic of Latvia No 560 "Guidelines for e-Health in Latvia"// with amendments announced till 13.06.2006. Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 131, 19.05.2005.
[17] 15.02.2007 Working document No 131 "Working Document on the processing of personal data relating to health in electronic health records (EHR)" adopted by Working Party set up under Article 29 of Directive 95/46/EC of the on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://www.bfdi.bund.de/SharedDocs/Publikationen/Art29Gruppe/WP131_en.pdf?__blob=publicationFile
[18] 20.06.2007 Opinion No 4/2007 on the concept of personal data adopted by Working Party set up under Article 29 of Directive 95/46/EC of the on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
[19] WHITE PAPER. Together for Health: A Strategic Approach for the EU 2008-2013. Commission of the European Communities. COM(2007) 630, 23.10.2007. http://eur-lex.europa.eu/LexUriServ/site/lv/com/2007/com2007_0630lv01.pdf//.
[20] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. *Official Journal of the European Union* C 306.
[21] 17.12.2007 Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 82.
[22] 28.05.2008. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML.
[23] The Treaty on the Functioning of the European Union (consolidated version). *Official Journal of the European Union* C 115, 09.05.2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:EN:PDF.
[24] Commission communication "Telemedicine for the benefit of patients, healthcare systems and society", COM(2008) 689 final, 4.11.2008. (2009/C 317/15). http://ec.europa.eu/information_society/activities/health/policy/telemedicine/index_en.htm
[25] 17.12.2009 Law "On the Rights of Patients". Official Newspaper of the Republic of Latvia *Latvijas Vēstnesis* No 205, 30.12.2009.
[26] Directive 2011/24/EU of the European Parliament and of the Council on the application of patients' rights in cross boarder healthcare. *Official Journal of the European Union* L 88, 04.04.2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF.
[27] Judgment of the Department of Administrative Cases of the Supreme Court Senate of the Republic of Latvia. Case No SKA-347/2010, 01.07.2010.