analesdepediatría

www.analesdepediatria.org

SPECIAL ARTICLE

The responsibilities arising from the use of information and communication technologies in health professional practice☆

Laura Muñoz Fernández[a], **Elena Díaz García**[b], **Sergio Gallego Riestra**[a,*]

[a] *Consejería de Salud del Principado de Asturias, Oviedo, Spain*
[b] *Servicio de Salud del Principado de Asturias, Oviedo, Spain*

Received 3 March 2020; accepted 5 March 2020
Available online 10 May 2020

KEYWORDS
ICT;
Information and communication technologies;
eHealth;
Professional responsibility;
Telemedicine;
Digital consultations;
Health 2.0;
Data protection

Abstract The increasing use of Information and Communication Technologies (ICT) in the health setting has given rise to the current phenomenon of eHealth or eMedicine, terms equivalent to the cyberspace concept, but refer exclusively to health. Due to the appearance of Web 2.0 it can be stated that we are dealing with a phenomenon much greater than just using the technologies: we are facing a real social change, giving rise to that called Health 2.0.

The legal regulation of this cyberspace requires two different types of rules. Some that regulate cyberspace itself, and others, the actions performed with its use and to those that appear applicable to conventional law. In this latter case, we are referring to the applying of already existing laws to actions performed using ICT, as is the case of medical actions.

Within these latter situations, two clearly different ones have to be distinguished: the professional responsibilities arising from medical actions carried out within health organisation settings when the use of ICT is introduced, and those other actions carried out voluntarily, individually and privately, using personal media and devices. It is in these types of actions where the legality, as regards data protection and privacy of the patient, appears to be violated, and at the same time the professional may be held responsible.

☆ Please cite this article as: Muñoz Fernández L, Díaz García E, Gallego Riestra S. Las responsabilidades derivadas del uso de las tecnologías de la información y comunicación en el ejercicio de las profesiones sanitarias. An Pediatr (Barc). 2020;92:307.

* Corresponding author.
E-mail address: sergiomauel.gallegoriestra@asturias.org (S. Gallego Riestra).

PALABRAS CLAVE
TIC;
Tecnologías de la Información y Comunicación;
eSalud;
Responsabilidad profesional;
Telemedicina;
Interconsultas digitales;
Salud 2.0;
Protección de datos

Las responsabilidades derivadas del uso de las tecnologías de la información y comunicación en el ejercicio de las profesiones sanitarias

Resumen La evolución de las tecnologías de la información y comunicación (en adelante TIC) en el ámbito sanitario ha dado lugar al fenómeno actual de la eHealth o eSalud, términos equivalentes al concepto de ciberespacio, pero referido exclusivamente a la salud. Fruto de la aparición de la web 2.0 se puede afirmar que nos encontramos ante un fenómeno mucho mayor que lo que sería el mero uso de tecnologías: estamos ante un verdadero cambio social dando lugar a la denominada Salud 2.0.

La regulación jurídica de este ciberespacio exige 2 tipos distintos de normas. Unas que regulen el ciberespacio en sí mismo y otras los hechos que se realizan con el uso del mismo y a las que parece aplicable el derecho convencional. En este último caso nos estamos refiriendo a la aplicación del derecho ya existente a los actos realizados a través de las TIC, como es el caso de los actos médicos.

Dentro de estos últimos también hay que distinguir 2 situaciones claramente diferentes: las responsabilidades profesionales derivadas de actos médicos ejecutados dentro del ejercicio profesional, llevado a cabo en el seno de las organizaciones sanitarias cuando se implanta el uso de las TIC y aquellos otros actos ejecutados de manera voluntaria y a título individual y privado, utilizando medios y dispositivos propios. Es en este tipo de actos donde la legalidad se ve generalmente conculcada respecto a la protección de datos y la intimidad de los pacientes, y a la vez los profesionales pueden incurrir en responsabilidades.

Current framework

Society is currently living a momentous shift related to information and communication technologies (ICTs) brought by the sustained increase in the capacities of computation, data storage, content generation and the speed of data exchange. This has resulted in a veritable social transformation: ICTs are changing the way in which we relate to each other, work, or spend our leisure time. The most powerful drive of this change may have been the advent of the Web 2.0 or social web, defined by Tim O'Reilly in 2005 as the network as platform, spanning all connected devices, creating network effects through an architecture of participation. Counter to what then came to be known as the web 1.0, which was designed as an information container, the Web 2.0 allows users to interact and collaborate, who become active rather than passive users with the ability to participate, create contents, support and be part of societies and/or communities at different levels.[1] Rather than a technological shift it was a shift in the approach to traditional technology applications, which started focusing on the user. This is what led to the well-known digital transformation that involves the active and voluntary participation of users, but also passive involvement, that is, the induced involvement or dragging of other subjects that range from natural persons to organisations, associations and states.[2]

In the health care field, after the initial introduction of computing systems in the 1970s, we have progressed from medical computing to eHealth or telehealth. Medical computing is limited to combining medical science with several fields of information and computer science to attempt to improve patient care. However, eHealth or telehealth goes beyond this, as it involves a broader use of ICTs in health care, including their application in systems and tools for patient management, research, education of health professionals, disease monitoring and public health surveillance,[3] reaching what, due to similarities with its web counterpart, has been termed health 2.0, a new approach to health care that takes advantage of the possibilities offered by the Web 2.0.

In this new framework, patients have evolved into ''technopatients'', ''digital patients'', ''empowered patients'' or even ''impatients'': patients with a proactive attitude towards their health and/or disease that search information online and through social networks, who demand more information from health providers and participate in decision-making regarding their health.[4]

Thus, there is no question that the emergence of the Web 2.0 has been an enormous breakthrough in the accessibility of information, freedom of expression and the ease and fluidity of interpersonal communication, but it is just as clear that it has been accompanied by the emergence of very significant risks regarding personality rights, individual and family privacy, personal image and data protection. Along with these general risks have emerged risks specific to the particular activities carried out digitally, especially when it comes to professional activities such as the practice of medicine. We are facing a phenomenon that goes

well beyond the mere use of technology, a true social shift that includes behaviour patterns that challenge the validity of current laws and regulations to manage the situations that come up and make us question the extent to which current law can be directly applied to these new circumstances.

The development of ICTs that allow the interconnection of individuals has given rise to what is known as cyberspace. The cyberspace is defined by Barrio Andrés as ''the global space in the framework of the Information Society consisting of the interdependent set of ICT infrastructures that include the Internet, telecommunications networks, and the integrated computing systems, processors and controllers that constitute the Internet of Things''.[5] The regulation of this cyberspaces poses a challenge to the law and requires two forms of legal structures. On one hand, cyberspace itself must be regulated as a new entity that has not been subject to the law, as should be the actions carried out in cyberspace and to which conventional law applies. With the latter we refer to the application of current law to actions carried out through ICTs but that could have juridical consequences by being actions with space and time boundaries, such as medical interventions performed in cyberspace but nevertheless in a specific and clearly defined space and involving subjects that are perfectly identified.

The need to provide cybersecurity through law is expressed by the new European Union regulation on personal data protection,[6] as it specifies that the law must cover the necessary free flow of such data. The text of this regulation evinces that the advance of technology and globalization pose new challenges for personal data protection, as its collection and exchange have grown significantly, and it highlights that interoperable formats must be used to enable data portability. It emphasises that technology allows both private companies and public authorities to make use of personal data on an unprecedented scale, while natural persons increasingly make personal information available publicly and globally, developments that require a stronger legal and practical data protection framework for natural persons, economic operators and public authorities.

With the issue framed in these terms, we assume that the regulation of cyberspace will develop gradually with new and specific laws. When it comes to the application of current law to specific and well-defined acts performed in cyberspace, the text differentiates between two clearly different situations in the use of ICTs: the professional responsibilities derived from health care actions carried out in the course of professional medical practice in the framework of health care organisations and actions carried out voluntarily on a private and personal basis.

Potential responsibilities derived from the introduction of ICTs in the health care system

It has been years since the public health system started to implement health care services using ICTs, giving rise to different modalities, among which we ought to highlight teleinterconsultation and telediagnosis, whose purpose is to assess a disease or a previous diagnosis through the exchange of information, including images, between health care professionals. The umbrella of telemedicine encompasses teledermatology, telecardiology or teleophthalmology, fields with procedures that have been integrated in the public health system with the approval and encouragement of the competent authorities. Another particular characteristic of these services is that they are carried out with means provided by the public health administration and that rules have been established for their implementation.

This set of techniques is widely known as telemedicine. Twenty years ago, the World Health Organization (WHO) defined it as ''the delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities.''[7] On its part, the World Medical Association (WMA), also 20 years ago, considered that ''telemedicine is the practice of medicine, from a distance, in which interventions, diagnostic and treatment decisions and recommendations are based on clinical data, documents and other information transmitted through telecommunication systems.''[8] The WMA noted that telemedicine should be used exceptionally and only in cases where the physician is unable to be physically present within a reasonable time and under adequately safe conditions, or, in other words, that face-to-face personal interaction within the patient-physician relationship should be maintained whenever possible.

As we can see, telemedicine was initially conceived as an approach strictly associated with enabling the provision of services where distance was an issue. However, the concept has gradually expanded to approximate the current notions of globalization and interoperability that we have referred to above in the context of the new European Union regulation. The ethical debate spurred by the practice of telemedicine from its inception concerns whether it should only be practiced in case of emergency or when physical distance precludes face-to-face care, or whether its practice should be accepted as an alternative to conventional medicine. It appears that the latter is the trend that is prevailing, as it allows better use of resources, offers clear management advantages and it has been demonstrated that certain artificial intelligence-assisted applications are very reliable for diagnosis.

The use of telemedicine, under any and all circumstances, must be held to minimum standards. As early as 2002, Sánchez Caro and Abellán[9] established requirements that ought to be fulfilled for practicing telemedicine without incurring responsibility (Table 1). We could summarise them as follows:

Table 1 Requirements for practicing telemedicine without incurring responsibility.

The use of telemedicine is justified by the benefit to the patient, but never by exclusively increasing convenience for the physician
Consent must be obtained from the patient, and the provider needs to adhere to security regulations to ensure the confidentiality of the patient
All aspects concerning each case must be properly documented and preserved in the health records, attempting to guarantee permanent storage of the data, ensuring its security and safe retrieval
Professionals that practice telemedicine interventions must be accredited to practice in the country where they operate and be competent in the medical speciality that they practice

1) The use of telemedicine is justified by the benefit to the patient, but never by exclusively increasing convenience for the physician.
2) Consent must be obtained from the patient, and in order to avert the data breach risks involved in electronic communications, the provider needs to adhere to security regulations to ensure the confidentiality of the patient in 2 aspects:
   - Patient-related data and other data concerning the patient cannot be shared with another physician or health care provider unless requested or authorised by the patient, and it can only be shared to the extent that the patient allows.
   - Any shared information has to be related to the specific medical issue at hand.
3) It is important to properly document and record all aspects concerning each case in the health records, attempting to guarantee permanent storage of the data, ensuring its security and safe retrieval.
4) Professionals that practice telemedicine interventions must be accredited to practice in the country where they operate and be competent in the medical speciality that they practice. The anticipation of this requirement by these authors nearly 20 years ago is remarkable considering today's emphasis on applying territorial law to actions conducted in cyberspace.

The 2011 Medical Code of Ethics has addressed the issue of telemedicine, covering its practice and establishing considerations that can be standardised into the following rules (article 26):

- The clinical practice of medicine by consultations exclusively performed through postal mail, telephone, radio, printed materials or the internet goes against the code of ethics. Appropriate practice inescapably entails direct, face-to-face contact between patient and physician.
- It is ethically acceptable, in case of second opinions and medical check ups, to use email or other means of distance communication and telemedicine, as long as the provider and patient are mutually and clearly identified, and privacy is guaranteed. Patient guidance systems that use telephone consultations or telemedicine conform are ethical as long as they are used exclusively to assist in decision-making.
- Telemedicine is bound to the same confidentiality, safety and privacy regulations established in relation to conventional medicine in the Code of Ethics.
- The clinical practice of medicine by consultations exclusively performed through postal mail, telephone, radio, printed materials or the internet goes against the code of ethics, but these vehicles may be used to provide guidance or assist in decision-making.

In light of the progressive growth of social networks, in 2014 the Spanish Board of Physicians published a Style Manual for health care professionals on the use of social networks.[10] Based on the content of the aforementioned article 26 of the Medical Code of Ethics, it developed a chapter titled ''Medical advice for virtual patients'' (Chapter 2) that we strongly recommend reading.

All the above requisites are obligatory conditions that health care organisations must guarantee when establishing telemedicine programmes, while the responsibility of professionals will be limited to their professional practice. It is obvious that physicians cannot be held liable for security violations in data protection, losses of relevant data or errors in health care delivery resulting directly from the technologies used. Their responsibility is strictly limited to the health care intervention that they carry out, with no differences relative to the responsibilities derived of the practice of conventional medicine.

Potential responsibilities derived from the voluntary use of ICTs on a private, personal basis outside the framework of the health care system

Along with the introduction of telemedicine at the institutional level, telehealth and virtual visit services are emerging in which the relationship does not involve health care professionals within an organised health care system that is responsible for the medium used for the purpose, but the direct interaction of patient and provider, usually through the private use of vehicles outside the channels and tools established by the health care institution. The use of open social networks should be ruled out, as they do not constitute an adequate means to maintain a professional relationship, as they do not allow accurate identification and are not trustworthy environments.[11]

First of all, we ought to note that the use of private devices for storage and transfer of health information brings up serious concerns regarding legality, but it is just as important that the potential reach of this type of actions is understood, along with the responsibilities that they may entail. The use of email and instant messaging systems such as WhatsApp to exchange information regarding patients with identified or identifiable health information is an illegal practice that directly contravenes current regulatory law. Thus, Royal Decree 1720/2007, of December 21, which approves the Regulation for the implementation of Organic Law 15/1999, of December 13, on the Protection of Personal Data[12] (a law that is still in force), stipulates the security measures that must be in place in this type of services and specifically establishes that the storage of health-related personal data in computer systems requires high-level security measures. These include the duty to make back-up copies, control access to the data and keep an access record for 2 years. In addition, the decree stipulates that processing of personal data in portable devices that do not allow encryption should be avoided, and that transfer of health-related personal data through public or wireless electronic communication networks shall be done by encrypting the data or by using any other mechanism that will guarantee that the information will not be intelligible or manipulated by third parties, something that is clearly not fulfilled in the hypothetical use of email or WhatsApp that we have previously described.

Public networks are those where individuals can obtain services. Private networks are institution networks such as the intranet of the Ministry of Health or the National Health System or the Public Administration of Spain. Thus, public health organisations use these private intranets to develop their telemedicine projects and any other activities that involve interoperation, such as nationwide projects like the electronic prescription and the electronic health records databases of the National Health System. In short, the storage and the transfer of health data by health professionals outside these systems, that is, through mobile phones, private computers, tablets etc. and through wireless and public networks would require the use of encryption software and security measures that cannot currently be applied to these devices.

When the exchange of personal health data is carried out by patients themselves or their legal representatives, it could be assumed that the interested party has consented to this exchange. We are not referring to the concept of implied consent but to the manifest and express consent intrinsic to the act of patients submitting their own data to obtain guidance on their health problems from a health care professional. This excludes the possibility of health care providers initiating this type of electronic exchange with patients and submitting test results or recommendations regarding their health problems, which would be illegal unless the provider had received express consent and was able to furnish proof of it. We are referring to the growing practice of maintaining electronic contact with chronic patients to provide on-demand guidance on what they need to do. In these cases, it could be argued that there is no infringement of data protection laws, yet the advisability of such practices remains highly questionable. If we wish to apply current positive law to these exchanges, the first question that arises is whether this type of actions fall in the scope of employment and the employer in this case the Public Health Administration, would be liable for the actions of the employee, when they are neither known nor authorised by said administration and are carried out through private devices and unbounded by any form of regulation. In other words, are these health care actions? Would the civil liability insurance of the Administration cover a harmful event derived from this form of electronic interaction? Should public funds be used to pay compensation in these cases? And when the Public Health Administration has been held liable as the employer of the health provider, should it pursue compensation from the health provider? There do not seem to be many encouraging answers for health professionals in this type of scenario in which the answers are immediately obvious.

Conflict of interest

The authors declare that there are no conflicts of interest.

References

1. Web 2.0. Wikipedia. Available at: https://es.wikipedia.org/wiki/Web_2.0 [accessed December 2019].
2. Hoffman-Riem W. Big Data. Desafíos también para el derecho. Cuadernos Cívitas; 2018.
3. Monteagudo Peña JL. El marco del desarrollo de la e-salud en España. Área de investigación en telemedicina y sociedad de la información. Madrid: Instituto de Salud Carlos III; 2001.
4. Sánchez-Caro J, Abellán-García Sánchez F. El paciente (impaciente) del siglo XXI. In: Sánchez-Caro J, Abellán-García Sánchez F (Coords), editors. Avances en salud: aspectos científicos, clínicos, bioéticos y legales. Fundación Merck Salud; 2018. p. 219–34.
5. Barrio Andrés M. Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza en Internet. Valencia: Tiran lo Blanch; 2018.
6. Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1–88.
7. Plan de telemedicina del INSALUD. Área de estudios, documentación y coordinación normativa. Madrid; 2000.
8. Toma de posición de la Asociación Médica Mundial sobre las responsabilidades y las directrices éticas ligadas a la práctica de la telemedicina, adoptada por la 51 Asamblea, celebrada en Tel Aviv (Israel), en octubre de 1999. Actualidad del Derecho Sanitario. 2000;62:481–4.
9. Sánchez Caro J, Abellán F. Telemedicina y protección de datos sanitarios. Granada: Fundación Salud; 2000. p. 2002.
10. Organización Médica Colegial. Ética y Redes Sociales. Manual de estilo para médicos y estudiantes de medicina. Sobre el buen uso de las redes sociales. OMC. Consejo General de Colegios de Médicos de España. Available at: https://www.cgcom.es/sites/

default/files/u183/Manual%20Redes%20Sociales%20OMC.pdf [accessed January 2020].
11. Bataller A, Cassasa A, de Carreras LL, Martínez M, Moro M, Pidevall I, et al. Recomendaciones sobre el uso de información médica y el ejercicio de la libertad de expresión en las redes sociales. Consejo de Colegios de Médicos de Cataluña. Available at: https://www.comb.cat/Upload/Documents/7778.PDF [accessed January 2020].
12. España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17. pp. 4103–4136. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979&p=20120308&tn=1 [accessed January 2020].