Clinical Case Reports International

Review Article
Published: 27 Jul, 2019

Medical and Legal Aspects of Telemedicine in Ophthalmology

Gianfranco G[1] and Mauro S[2]*

[1]*Department of Sense Organs, Sapienza University of Rome, Italy*

[2]*Department of Medicine and Dentistry, Sapienza University of Rome, Italy*

Abstract

Telemedicine can provide adequate medical assistance for physically distant patients utilizing the joint adoption of Information and Communication Technologies. Telemedicine is the set of techniques and tools for health monitoring and cares implemented through systems providing rapid access to both specialists and patients, regardless of where they are located respectively. We live in the age of communication, and we have long had the problem of how to improve health in health systems. Telemedicine seems to be a viable alternative in order to eliminate the gap between human and economic resources. Due to its characteristics, it can contribute to improving access to specialized healthcare and the quality of life of people, especially in populations lacking qualified personnel, in remote or difficult access areas or patients with chronic diseases, by reducing long waiting lists and high costs for the health systems. While the telemedicine projects between different countries are developing more and more, the inherent ethical and legal problems are emerging at the same time. This article refers to telemedicine as a broad concept, including several types of distance medicine, thus identifying its strengths and weaknesses that will be the primary purpose of the medical-legal aspects. We will also describe its application in the ophthalmological field and the main issues raised by its implementation.

Keywords: Telemedicine; Ophthalmology; Medical Ethics; E-Health; Telecare

Telemedicine

Telemedicine is, according to the Commission of the European Communities, the provision of welfare services by using Information and Communication Technologies (ICT) in situations where the health professional and the patient (or two professionals) are not in the same location. It involves the reliable transmission of medical information and data thanks to texts, sounds, and images necessary for the prevention, diagnosis, treatment, and subsequent monitoring of patients [1]. Telemedicine has numerous benefits for doctors, medical institutions, and patients [2]. In this way, it plays a pivotal role in the development of medicine and the provision of health care in the world. Telemedicine allows remote group collaboration between health professionals in different places, even from different countries. It is useful for real-time interaction among the participants without a time interval between interventions. Professionals in distant positions can communicate, thus improving the quality of health services. The continuous flow of communication among health professionals is necessary due to the increasing complexity of medicine that prompts the doctors to consult with colleagues or experts in a particular issue or to need a second opinion. All these behaviors are considered good medical practice (considering that they will not delay an urgent procedure nor constitute a defensive medicine), and the absence of such contacts may be considered as lack of interest and attention by the doctor. On the other hand, today patients, who are aware of their rights and attentive to the risk of medical errors, also seek a second opinion, sometimes from doctors who have never really met, by using the telephone, the mail or even a website. In the perspective of health institutions, telemedicine opens up the possibility of expanding the spectrum of available medical services, thus increasing the chances of earning and saving. Furthermore, it can be quite convenient for the patients themselves. Telemedicine facilitates direct patient access to a distant doctor, without requiring the movement of any of the participants and allowing access to some forms of medical care that would otherwise not be available. Telemedicine can be an important tool in cases where geographical distance hinders access to health care, in particular, specialized healthcare, such as in many rural areas or in developing countries with the lack of health infrastructures [3-6]. Medical treatment in these scenarios would require long journeys, not always possible and usually rather

OPEN ACCESS

Correspondence:
Gianfranco Gioia, Department of Sense Organs, Sapienza University of Rome, Viale del Policlinico, 155, 00161, Rome, Italy, Tel: +393294180453; E-mail: gioiag86@hotmail.it

Received Date: 19 *Jun 2019*
Accepted Date: *23 Jul 2019*
Published Date: *27 Jul 2019*

Citation:
Gianfranco G, Mauro S. Medical and Legal Aspects of Telemedicine in Ophthalmology. Clin Case Rep Int. 2019; 3: 1110.

expensive, time-consuming and exhausting both for doctors and patients. Therefore, patients in this situation do not access to adequate health care. Telemedicine can also be a potentially very useful tool in preventive medicine, providing patients with useful information on their health conditions. It can be used for the monitoring of chronic conditions such as diabetic retinopathy, glaucoma, age-related macular degeneration, etc. that are growing public health problems due to the increasing life expectancy and elderly population. These diseases are also increasing in the young population. By means of telemedicine, we do not need to visit the patient in the hospital setting, but we use a telemonitoring [7] thus avoiding long waiting lists. Moreover, it is convenient to reduce hospitalization and health care costs. Telemedicine also has enormous potential as regards the electronic prescription in order to avoid errors, such as mistakes in the tax code, the patient's age or the dosage, consequently to incomprehensible calligraphy of the doctor [8]. The improvement of healthcare is the advantage of telemedicine. This goal materializes by means of the patient health education, the technical education of health workers by using the new e-learning technologies, and the ease of accessing a second opinion from a specialist, particularly important for people in rural areas or those who suffer from rare diseases. Notwithstanding all these advantages, telemedicine is not present in Europe. The difficulties of application are the huge costs of a telemedicine service, the difficult interoperability of technical infrastructures across countries, the privacy of health data, the lack of specific ethical standards and regulations for telemedicine, the doubts for healthcare professionals about their responsibility, and the uncertainties of the legal framework all over the world [9].

Telemedicine and Ophthalmology

Telemedicine has multiple applications in ophthalmology because it needs visual images for the screening, diagnosis, therapy, and monitoring of the diseases. It is not surprising that ophthalmology has been so quickly adapted to changes in the cybernetic world and that it uses the telemedicine technologic system in order to access to advanced healthcare. Its practical use has shown clinical, economic, and public health benefits [10,11]. For example, its use in two important pathologies, such as Diabetic Retinopathy (DR) and Retinopathy of Prematurity (ROP), shows how telemedicine can improve access to high-quality health care in these and other ophthalmological diseases. Although effective treatments for high-risk DR exist for over four decades, DR remains a major cause of blindness among adults of working age. The telemonitoring of DR is now one of the helpful specific applications of the telemedicine.

On the other hand, the inability of half of the population to timely access the exams has contributed to the increase of diabetes. The telemedicine programs provide access to the annual screening of DR patients through patient imaging in a setting of primary assistance. These programs have improved clinical outcomes [12,13].

Consequently, the spreading of the ophthalmological programs into the medical system would probably result in a suitable timing in eye care in the proportion of patients who did not access to retinal screening or eye tests with the appropriate frequency [14]. Image-based diagnosis and telemedicine have proven to be reliable, accurate, and cost-effective for ROP and improve access to eye care for premature babies at high risk for ROP [15,16]. The diagnosis and treatment of ROP are essential for successful results. There are doctors experienced in indirect ophthalmoscopy and trained in screening for ROP that can provide care for low birth weight infants. Telemedicine offers an interesting alternative, especially in the most remote areas.

Furthermore, imaging could improve the documentation of the retinal fundus. In this sense, telemedicine can successfully improve and extend ophthalmologic care using imaging technology. Other areas of telemedicine in ophthalmology are intraocular pressure monitoring, optic nerve analysis, macular disease monitoring, visual field analysis, and anterior segment diagnosis. Furthermore, the ability to perform remote consultations and examinations, instead of face-to-face, is gaining ground thanks to improved two-way communication technologies in emerging clinical institutions [17].

The Legal Framework of Telemedicine

As a health service, telemedicine is included in the scope of articles 56 and 57 of the Treaty on the Functioning of the European Union (TFEU); therefore, it is a service, and it is subject to the general freedom concerning the free movement of services. Nonetheless, this is not the only set of rules applicable to telemedicine within the European legal system. In fact, within the framework of European law, telemedicine is both a health service and an information service (a service normally provided for a fee, at a distance and electronically at individual request). Therefore, both regulations are applicable: those relating to health care and those relating to information society services [18].

As far as information and telecommunications are concerned, we must take into consideration the following documents: Directive 95/46/EU [19], the Data Protection Regulation (GDPR) [20], Directive 98/34/EC, the Information Society Services Directive [21,22], Directive 2000/31/EC, directive on electronic commerce [23], Directive 2002/58/EC and the directive on privacy and electronic communication [24]. About health services, the most relevant result for regulating this sector is Directive 2011/24/EU on the so-called cross-border directive [25]. Furthermore, the European Union (EU) has developed an important series of initiatives over the years in order to increase the use of telemedicine in Europe. These initiatives aim to transform telemedicine into a standard medical service, accessible to all European patients and fully covered by the respective social security system [26]. The EU's efforts are also quite economically significant, as the EU has invested over € 500 million in research funding on the development of eHealth instruments. However, the undeniable value of telemedicine should not hide its many difficulties, some of which are also present in traditional medicine, but which assume a new complexity within telemedicine. For example, when health workers from different countries and different languages collaborate, there is no consensus on language to use for data recording in the patient's medical record or who is responsible for providing technical training (the so-called e-literacy) to health professionals using new communication technologies. All electronic health records (EHRs) need to integrate into a global eHealth infrastructure that is accessible from every point in the EU. Despite several working documents and position papers issued by the European institutions, we still lack a uniform set of rules to regulate telemedicine in Europe. Most of the regulatory competences in these areas still depend on the Member States, retaining the best skills in health care and medicine. However, the problem is that the approach to telemedicine varies immensely among European countries, including the perspective chosen to regulate telemedicine: some states have approached telemedicine from the point of view of the laws in the field of ICT technologies, while other laws regard the health care domain or even the social security field. Therefore, even at the national level, there are legal

voids that threaten the practice of telemedicine, leaving unprotected patients and health workers [27].

The General Data Protection Regulation (GDPR): Privacy in Health

Published in the European Official Journal on 4 May 2016, it entered into force on 24 May 2016, but its implementation took place after two years, therefore starting from 25 May 2018. Regulation 2016/679 is European legislation about data protection. Since it is a regulation, it does not need for transposition by the Member States of the Union and will spread in the same way in all the States of the Union without margins of freedom in adaptation. Its purpose is the definitive harmonization of the regulation on the protection of personal data within the EU. With the Lisbon treaty, the protection of personal data has become a fundamental right of citizens, and therefore to be guaranteed in the same way throughout the territory of the union. By increasing citizens' trust in the digital society, thanks to the more stringent protection, the regulation is functional to the digital development of the EU and safeguards the free movement of personal data. With the European regulation, we move from a proprietary vision of the datum (not treatable without consent) to a vision of control of the data that favors the free circulation, at the same time strengthening the rights of the interested party. There is a fundamental right of patients to the confidentiality of their information and medical records. Patient privacy should be observed unless it is revoked (i.e., informed, non-coercive) in rare cases in which it neutralizes the public interest. The information disclosed should be limited to such information or part of the medical record. Telemedicine creates special problems due to the involvement of non-clinical staff in teleconsultations, and the vulnerability of transmission lines to security breaches. Legislation and guidelines do not apply to anonymous information stripped of all attributes that can identify the owner. This simple distinction between the two types of information apparently is not so clear in practice. The processing of health data is subject to a specific discipline. It is carried out by healthcare professionals (excluding orthopedists, dental hygienists, nurses, obstetricians, physiotherapists, and speech therapists), and public health organizations [20]. The confidentiality needs to guarantee for citizens in health facilities, and the health data relating to them. Health data are data subject to special treatment, as it can reveal very intimate details of the person, and, for this reason, there is a general prohibition of dissemination, as well as enhanced protection, of such data (Article 4 GDPR) [20]. Health data is all that personal information suitable to reveal a person's state of health and body and mental conditions. Genetic data and photographs taken for surgical interventions or controls are also health data. Furthermore, as established by the Court of Cassation (Civil Cassation, United Sections, judgment 12.27.2017, number 30981), sensitive data suitable to reveal the state of health must be treated with organizational methods to protect them, such as encryption thus making the data subject unidentifiable. The European regulation provides that health data can be used only for purposes related to health (treatment purposes), for the supervision of the National Health System and research in the public interest. These purposes allow the possibility to introduce special conditions or additional limits for treatment. In this sense, the Italian legislator has provided, with the new Privacy Code, further measures to protect health dataset by the national control authority and reviewed every two years. The article 9 (letter h) of the GDPR does not provide the consent of data processing for purposes of preventive medicine or occupational medicine, such as assessment of the employee's ability to work, diagnosis, assistance, management of health, on the basis of Union or Member State law or in accordance with the health professional contract. However, the rule allows the Member States to maintain or introduce additional conditions, including limitations concerning the processing of genetic data, biometric data, or health data. The Italian legislator, with the decree to update the Privacy Code, has introduced the possibility that the Guarantor imposes specific guarantee measures (additional to the normal security measures) for the treatment of health data [28]. The directive 680 of 2016 is similar to the GDPR. Many of the rules contained are similar or equivalent to those of the new European regulation on privacy and personal data. They have a specific scope of application and concern the processing carried out by the competent authorities for prevention, investigation, detection, and prosecution of offenses, execution of criminal penalties, safeguarding and preventing threats to public security. This directive expresses the need to keep the data for the time necessary to achieve the purposes and to review the data to verify the need for storage or deletion after the deadline. About the safety of the treatment, the appointment of the data protection officer is also obligatory for the judicial authority thanks to the assistance that this figure can provide in the management of complex treatments and sensitive data. As regards the violation of the new rules, the text provides for administrative sanctions against violations concerning the methods of processing and introduces penal sanctions for the treatment operated with illegitimate purposes [24].

The Informed Consent

Before proceeding with data collection, it is necessary to provide the information to the patient (if necessary, it is possible to provide orally even if it is preferably written). The document indicates the subject collecting data, the purposes of the treatment, the methods of treatment, the mandatory or optional nature of the provision of data, the subjects or the categories of subjects to whom the data can be communicated, the identification details of the holder, and the methods for exercising the rights to protect your data. The Italian Ophthalmological Society has elaborated, in addition to the Guidelines, the Informed Consent Forms that regulate and define the criteria for the development of the main activities of the ophthalmologist. Informed consent is the tool through which information is disposable for the patient about the intervention and is gathered his consent to proceed. Therefore, it presupposes two distinct moments: information and then the actual consent. The Informed Consent consists of documentation: the specific information sheet of the intervention about the execution procedure, the post-treatment, advantages, disadvantages, risks, and complications. The Act of Consent remains the same for all the information sheets and does not need any specificity linked to the treatment [29]. The article 1, in compliance with the principles, set out in articles 2, 13 and 32 of the Law 219/2017 of the Constitution, states that no medical treatment starts or continues without the free and informed consent of the interested person, except in cases expressly provided by law [30]. However, the possibility of carrying out the treatment according to the public interest remains (for example, data processed to allow the study of a disease in order to treat other people). The Italian legal system provides for the freedom of choice of the place of care (article 32 of the Constitution and Legislative Decree 502/92) and the freedom to undergo treatment or not (Article 1 of Law 219/2017). According to the GDPR, once the city has decided to undergo treatment, they cannot refuse consent to the processing of data for treatment and diagnosis purposes. The digital preservation process aims to make

a document usable over time in all its integrity and authenticity, in its "digital essence" and in full compliance with the new privacy regulation (European Regulation 679 on protecting personal data) [20]. The Digital Administration Code asserts that the Information Technology (IT) document and its processing are valid and relevant for the law and recognizes the equivalence between a computerized and paper document. Decree of the President of the Council of Ministers of the Italian Republic (DPCM) of 13 November 2014 sets the technical rules for the formation of the IT document. DPCM of 3 December 2013 preceded it, published in the Official Gazette number 59 of 12 March 2014 and related to managing IT documents and their preservation. The technical rules on preservation introduce adaptation to international standards and national standards [31,32].

The Electronic Sanitary File (ESF)

The ESF, provided by article 12 of legislative decree 179/2012, is an IT tool that combines data and documents (digital or digitized) of health and social-health type related to the patients. Its function is to share such data and the patient's medical history among various doctors or health organizations. In addition to the patient (with safe modes, e.g., smart card), the ESF can access doctors and authorized healthcare personnel. Since the article 12 of Decree-Law 179/2012 is active, the inclusion of data within the ESF depends on the consent of the patient (article 3 bis). In this regard, you know about who has access to your data and how these data are used. The consent to the formation of the ESF is of course, quite distinct from the treatment. The lack of consent to the establishment of the ESF or the insertion of some data in the file cannot preclude the possibility of using the treatment. The patient has the right to revoke the consent and to obscure some specific data from the ESF. Although mobile electronic medical records are beneficial, several factors contribute to their not full potential use. Training in functionality and reliable infrastructures might foster tablet implementation [33]. The European Union of Medical Specialists (EUMS) has published a document that contains the "European Definition of Medical Act." This definition, adopted for the first time in 2005, was later amended in 2006 and finally in the Brussels meeting of 25 April 2009. This is the approved version: "The medical act covers all professional activities, for example of scientific, teaching, training, educational, organizational, clinical and medical technology, carried out in order to promote health, prevent diseases, make diagnoses and prescribe therapeutic treatments or rehabilitative treatments for patients, individuals, groups or communities, in the framework of ethical and deontological rules. The medical act is a responsibility of the qualified physician; it must be performed by the doctor or under his direct supervision and prescription." Patients who disclose personal information to their physicians must be able to trust them in order to protect the same information against other incidents to the treatment process. In this sense, there is no distinction between traditional medicine and telemedicine. The duty of confidentiality applies to all information provided to a tele-consulting doctor by a third party that may be a healthcare professional, aware of the patient-doctor relationship and under the same obligation of confidentiality [34].

The Information Disclosure Consent

Most patients understand that the primary physician responsible for their case will need to ensure that all team members have the information to fulfill their professional roles in the care process. When patients consent to the disclosure of information about them, it is necessary to ensure that they understand the reasons for disclosure. It is necessary to ensure that the patients are informed whenever information about them is likely to be disclosed to others involved in their health care and that they have the opportunity to retain information. If the doctor decides to divulge confidential information, he must be ready to explain and justify his decision. Because of the need to inform members of the support team, the law assumes the patient's implicit consent to disclose information to them. A final point concerns the circumstances in which the doctor or other authorities can cancel the patient's refusal to disclose. These circumstances arise when medical conditions of a patient pose a severe threat to the community in general. Health status data are visible to third parties, such as relatives, family members, voluntary personnel, after the patient, if conscious, has been informed and allowed. In any case, it is necessary to respect the request of the person hospitalized to not make known even to the legitimate third parties his presence in the health facility or information on his health conditions [35]. The issue of the access right to the patient's medical record obviously binds to the more general right of access to administrative documents (governed by the article 22 and following Law 241/1990) and to the treatment of personal health data according to the code about personal data protection referred to legislative decree number 196/2003. The public medical record is subject to the productivity of incident effects on subjective legal situations of public relevance (see Criminal Court, Section V, 21 November 2011, Number 42917). The prevailing doctrine attributes juridical relevance to the medical record, as it is the only instrument capable of processing patient care information to allow communication between the various health care workers. The doctor, in charge of compilation, is a public official pursuant to article 357 of the penal code, while the person responsible for the storage and good keeping is always the head of the department where the patient is undergoing treatment. The doctor has required a particular accuracy in writing all elements in the medical record: diagnosis, therapy, outcomes, etc. according to the article 24 of the Decree of the Minister of Health of 5 August 1977 and arranged according to the procedures set forth in article 26 of the Code of Medical Deontology. The medical record together with the related reports needs indefinite preservation, as it is an official act essential to ensure the certainty of clinical data, as well as being a valuable source of documentation for research of historical health data. In this panorama, the question of limits on access to third parties to the information contained in the medical record belonging to another subject has legal importance [36].

The Network and Information Security (NIS) Directive for Health Data Protection

Several devices are useful for remote communication, such as video conferencing unit, e-mail, webcam, Smartphone, etc. The channel to allow communication is variable (broadband, network, wireless). The legal perspective of confidentiality focuses on the relationship between the subjects involved rather than on the systems by which they communicate, but we must pay attention to this last aspect. We consider the NIS directive as the first step in the European cyber security strategy. Approved by the EU Parliament on 6 July 2016, the directive aims to reinforce the security and IT resilience within the Old Continent. The need for NIS directive starts from a consideration: networks, systems, and information services play a vital role in today society. Without them, the internal market could not work, so it is essential for their reliability and security for economic and social activities. The NIS applies to two categories: the operators of essential services that are necessary to the maintenance

of basic social and economic activities (such as health, transport and energy companies), and the digital service operators such as search engines, e-commerce platforms, etc. Both of them need to adopt appropriate technical and organizational measures to manage risks and prevent IT incidents. In the event of default, very severe penalties will be present, ranging from a minimum of 12 thousand up to 150 thousand Euros. In this regard, it is necessary, at the national level, the designation of an intervention group for cyber security in the event of an accident and national authority responsible for the security of networks and information systems. Furthermore, the NIS establishes the cooperation group composed of representatives of the Member States, the Commission and the European Network and Information Security Agency (ENISA), a team to promote collaboration between the countries of the Union in relation to the security of networks and information systems in order to facilitate the information exchange. The two regulations, i.e., the GDPR and the NIS directive, overlap when an IT security incident involves violation of personal data [37].

Electronic Identification Authentication and trust Services (eIDAS)

The eIDAS is the European regulation governing electronic signatures, money transfers, and other types of electronic transactions in the European single market. It has allowed the creation of standards for electronic signatures, digital certificates and other forms of electronic authentication, thus allowing for the replacement of paper documents with digital equivalents that have the same legal value and official recognition in all EU countries. The member countries of the EU are required to recognize electronic signatures that meet the standards set by eIDAS. In particular, it distinguishes three types of signatures inherent sensitive data. The director adheres with local, state, federal and international guidelines for the acquisition of health information, transmission and storage of data by interfacing with electronic medical records and widely available archiving and communication systems, preferably using standards-based interoperability protocols. Imaging performance and diagnostic acquisition devices in ophthalmology should follow periodic manufacturer's recommendations. Diagnostic displays need for periodic checking and recalibration for normal function. The security, integrity, and availability of data (including backup and archiving) are the tasks of the IT staff. The setting, i.e., a medical office, urgent care, emergency or community health care center, should be able to monitor the vital parameters of the test, to make a detailed medical history review, to conduct and transmit telemedicine for ophthalmological examination and to organize appropriate follow-up and care. Telemedicine exams will have different space requirements based on their use of synchronous technology or asynchronous technology. Synchronous visits require space for the patient, the local provider, and the remote provider to conduct the exam in private and discuss the results. Synchronous visits typically require audio and video equipment, a computer to transmit the necessary information about the exam and the devices and technologies to conduct a remote eye examination. Asynchronous visits require space for the necessary imaging equipment, other devices used, and space for the preparation and presentation of images and data. Generally, a small space within an existing clinical space is adequate for telemedicine examinations and consultations. There are few normative indications concerning the personnel who acquire, transmit, and interpret the data of telemedicine.

Each member of the team has the necessary qualifications established by the program. An activity-based (or "function-based") assessment of staff requirements is necessary. The reading method for image analysis should be transparent to the applicant. The reading center is responsible for reading errors. The basic requirements for staff involved in ophthalmology telemedicine in a remote imaging site are diagnostic equipment, the awareness of the risks and the clinical estimation of ocular complications due to pupillary dilatation (if imaging is under the mydriatic eyewash), universal precautions, antiseptic technique, and informed consent. Training for safe and correct contact with patients in a clinical setting, as indicated by applicable hospital and facility standards, is necessary. They are training on specific devices and equipment to obtain the necessary certifications and adherence to the quality control for the instruments are essential. The ophthalmologists who work as a distant doctor should receive initial training and periodic re-evaluation to meet quality standards for the activities performed. The doctor who reads the test must confirm the coverage of responsibility for medical negligence for this activity by the insurer. An expert reader, under the supervision of the physician, bases the current ophthalmology telemedicine on a store-and-forward model with image acquisition for subsequent evaluation. The most recent applications may involve home-based tests with transmission and web-based interactions by the patient [37].

Network Access, Data Transmission, Health Internet (Hi)-Ethics in Telemedicine

Telemedicine relies heavily on the video and audio transmission of data through telecommunications networks. Secure accesses to the network and data transmission are essential for the confidentiality of personal and medical data. The promise of this network is that patient information will be electronically available to authorized personnel wherever the patient is, or information is necessary. The access needs of at least one authentication check (password). The checks ensure that access is available only for authorized users. An appointed individual is responsible for the security of a connected system. All network workers are aware of their responsibilities. All the incidents threating the security are under control. The most obvious way to reduce the risk of unauthorized access to computer data on the Internet is to control traffic through the interface between the local network and the external Internet. This is a function of a firewall. It is important to know that they cannot protect themselves from the traffic that does not cross them. There are different types of firewalls such as the network-wide firewall using a router to make decisions, i.e. what to pass or block based on network protocols, usually Internet Protocol (IP) addresses, an application layer that is a system including a Personal Computer (PC) with two ports (one for entry and the other one for outgoing traffic). A firewall is a mean of ensuring that only the right traffic passes through.

Telemedicine includes four main areas:

- Live or synchronous audio-video telemedicine, i.e. bi-directional real time communication between a patient and a healthcare provider using audiovisual telecommunication technologies and data collection.

- Store-and-forward or asynchronous telemedicine (freely translatable as "store and return"), i.e. electronic transmission of health data (images, text or other digital data) to a healthcare provider for the evaluation and provision of the service using methods other than real-time interaction with the patient; it is a technique in which

an information, subdivided into packets in its path between the single stations (or nodes) of the network, must be totally received, before it can be retransmitted.

- Remote Patient Monitoring (RPM), i.e. collection of health data directly from the patient, usually during the normal activities of daily life, transmitted to a healthcare provider for analysis and possible actions.

- Mobile Health: health care, patient communication and training based on mobile communication platforms, e.g. mobile phones, tablets, PCs, etc.

Encryption is, therefore, a great help to protect telemedicine transmission. There are two types of encryption algorithms. With secret key encryption, the sender and recipient both use the same key to lock and unlock the message. On the contrary, with public-key cryptography, each user has two unique keys, i.e., a public key and a private key. In private, the key is useful to encrypt any message sent as a digital signature. The recipient can decrypt the signature with the public key to verify the identity and authenticity of the message. The power of digital signatures is that they also detect very slight changes in a message. Informed users naturally expect that the clinical information on the internet is high quality, accurate, timely, and evidence-based. Digital native users have less critical faculties. They are readily aware of the validity of what they read on the internet. Several organizations have tried to establish these principles in guidelines or codes of ethical practice for the construction of Internet sites. The Hi-Ethics consortium is a voluntary group aiming to join the websites and the most used health information providers whose goal is to gain consumer confidence in internet health services. The goals of Hi-Ethics are to offer internet services that reflect ethical and high-quality standards, to provide reliable and up-to-date health information, to keep private and secure personal information and to take special precautions for personal health information. The Hi-Ethics allows consumers to distinguish online health services following these principles from those that do not [38].

Telemedical Equipment and Operational Risks

There are two broad categories of equipment used in telemedicine for the ophthalmology program: information acquisition devices (camera, coherent optical tomography, tonometer, auto refractometer, campimeter, etc.), image communication devices (computers, servers, network devices, etc.) to send data. The remarkable technological development of biomedical equipment for therapeutic, rehabilitative and diagnostic use has certainly brought great benefits, but it has created, in the health structures, particular problems for the protection of personnel, patients and health workers, mostly from electronic risks. Before using any biomedical equipment, make sure it has undergone regular acceptance testing and that the operators have received adequate and specific training on its correct use. For a long time, the CEI EN 60601-1 standard has been the reference for manufacturers and users of electro-medical devices for the diagnosis and treatment of patients. The international work of adaptation of the norm in these last years, after some modifications published in 1991 and 1995, has led to the publication of the third edition in 2006 in which the concept of safety has been expanded to include the aspect of the essential performance of electromedical equipment. The experience also extends to the legal aspects of telemedical equipment. The basis of this legislative framework is the Consumer Protection Act of 1987 dealing with the general responsibility for artisanal products and applied to the teleconsultations equipment [39]. The regulations apply to Computed Tomography (CT) scanners, X-rays, ultrasounds, etc. All these devices (including new videoconferences and related equipment) must show the European Conformity (CE) mark indicating that they comply with the appropriate safety, quality, and performance standards. The Medical Devices Agency (MDA) is also responsible for registering the manufacturer and reporting incidents, as well as for the general implementation and promotion of European directives. MDA has identified the repeated causes of adverse incidents with medical devices such as poor quality, outdated or worn-out devices, and incompatibility with auxiliary equipment, poor documentation, inappropriate use, inadequate training, maintenance errors or lack of assistance. These comments mainly refer to the malfunctions of the operational equipment [40]. Several devices are useful to communicate remotely, such as a video conferencing unit, e-mail, webcam, or Smartphone. The channel allowing communication can be broadband, network, or wireless. The operational risks are those identified by the MDA as the main causes of adverse accidents. The analysis of these cases shows that they fall into two categories: inadequacies due to technology and those due to insufficient staff. We can distinguish four main technological risks involving:

- The image quality: a patient has the right to expect that a consultant can draw the same correct conclusions from an image on a telemedicine screen as from a conventional face-to-face visit, particularly important for Ophthalmology surveys.

- The lack of suitable equipment for a health service.

- Malfunctioning equipment: the breakdown of the computer or video equipment is unfortunately one of the most common features of telemedicine.

- Inadequate guidelines: Guidelines are as a bridge between technology and participants in teleconsulting. The guidelines determine the teleconsultation process and the documentation provides an archive of therapy, prescriptions, dosages of drugs, plans, etc. This combination of protocol and recording of the action provides a powerful audit trail that can have considerable value in any legal dispute.

In Italy, the Directorate General for Medical Devices and the Pharmaceutical Service is responsible for the completion and implementation of the regulation of medical devices, including tasks related to market surveillance, accident monitoring, clinical investigations, and evaluation of technologies and address of Health Technology Assessment (HTA) activities [41]. As regards the operational risks due to the staff, the Commission refers to the definition of "healthcare professionals" as defined in the article 3/f of the Directive 2011/24/EU [38]. Healthcare professional is the doctor, the nurse responsible for the general care, the dentist, the midwife, or the pharmacist according to the Directive 2005/36/EC. We have principles to ensure that each team member is aware of his responsibilities and those of the other members. The patient should also know who is responsible for his care. These are simple precautions to avoid complaints of negligence. Telemedicine has sensitized people on issues that underline legislative discrepancy about the problem of accreditation and qualifications of health staff to protect the patient from incompetent professionals [41,42].

Discussion

The benefits of telemedicine are promising and, mainly, in ophthalmology, that is a specialization based on diagnostic imaging. The application of telemedicine is useful for patients, for ophthalmologists and health institutions as it allows access to medical care, it avoids unnecessary long movements, and it increases the profits by reaching patients, by expanding the spectrum of available services and by reducing health care costs and waiting lists. Telemedicine in ophthalmology allows collaboration between professionals from different locations, sometimes even from different countries. It simplifies, through different telecommunications channels and mobile technologies, direct patient access to ophthalmologists who practice in another city or country without requiring any of the participants to travel. However, some characteristics of telemedicine can become problematic, such as the violation of privacy, the physical distance, the inclusion of new technological methods, the purchase of expensive equipment, the weakening of the doctor/patient relationship, the involuntary increase in opportunities for incorrect behavior, the delegation of functions due to the remote nature of the treatment process, etc. Health professionals should consider that telemedicine could lead them to face further potential medical errors within a substantially more challenging standard of care. The EU has not yet issued specific rules on medical liability, despite its specific features, and this gap can jeopardize the development of telemedicine in Europe, thus denying all its benefits to European patients. However, the EU will not be able to create a uniform regulation covering all aspects of telemedicine, but it has already taken a step forward in terms of technology and privacy, which are already well-defined topics under European law. As regards the rights of patients in the field of telemedicine, the EU will be able to create some basic guidelines in the context of cross-border healthcare patients' rights. The rights of European patients still lack a set of uniform rules and the standardization in such a complex area as telemedicine; perhaps it would not be the best choice. We cannot expect harmonized rules for the medical responsibility deriving from telemedicine. Member States have very different national laws to address these issues because the EU brings together models of continental law and common law models. Because of this intrinsic difference, the attempt to harmonize civil liability, especially criminal liability, will be doomed to fail. It would be the scope for each Member State to provide a legal framework for telemedicine, while the role of the EU would be limited to requiring the Member States to regulate it. Most of the legal issues we have considered so far tend to fall into two well-defined categories: problems that have a frequent basis with conventional medicine and those that are specific to telemedicine.

When telemedicine takes place across national borders, or in Europe, there is likely to be even more opportunity for legal discord on which laws to apply; i.e., the laws of the country where the telepatient is present or of the country where the teleconsultation took place. What happens if telemedicine is legal to practice in one country but is not in another? We need to confirm a telemedicine task force in ophthalmology involving the academic and research world by using excellent resources, and collaboration between the Italian Ophthalmology Society, the Italian Association of Doctors Ophthalmologists and the Society of Legal Medicine in Ophthalmology to establish the legislation and guidelines of the telemedicine. The health manager or health director of telemedicine is necessary to avoid the delegation of care to less qualified subordinates and to establish their competences and responsibilities. Telemedicine is not a defined discipline to justify the professional accreditation of "Ophthalmologist Specialist in Telemedicine." Tele-education or eLearning should become a standardized process with certification requirement as well as continuous courses are necessary to spread the current European legislation in telemedicine both at the Ministry of Health and Medical Orders levels in all Italian regions. In conclusion, it is a good investment of efforts and resources because the worldwide future of telemedicine in ophthalmology undoubtedly promises well.

References

1. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Telemedicine for the benefit of Patients, Healthcare Systems and Society. Brussels, 4.11.2008 COM (2008) 689 final, Commission of the European Communities.
2. Alsos OA, Das A, Svanaes D. Mobile health IT: the effect of user interface and form factor on doctor-patient communication. Int J Med Inform. 2012;81(1):12-28.
3. EHealth Stakeholder Group. Widespread deployment of telemedicine's services in Europe. Report of the eHealth Stakeholder Group on implementing the digital agenda for Europe. Key action 13/2 "Telemedicine"; Version 1.0 final (12 March 2014).
4. Kamsu-Foguem B, Foguem C. Could telemedicine enhance traditional medical practices. Eur Res Telemed. 2014;3(3):117-23.
5. Wamala D, Katamba A, Dworak O. Feasibility and diagnostic accuracy of Internet-based dynamic telepathology between Uganda and Germany. J Telemed Telecare. 2011;17(5):222-5.
6. World Health Organization. Telemedicine: Opportunities and developments in Member States: report on the second global survey on eHealth 2009. Geneva: WHO 2009 [cited 2015 Sep 10]. Global Observatory for eHealth Series; volume 2.
7. Gelein K. Are online consultations a prescription for trouble? The uncharted waters of cyber medicine. Brook L Rev. 2000;66:209-57.
8. Monteagudo JL, Munoz A, Pascual M, García-Sagredo P, Salvador C. La seguridad del paciente en telesalud: Una visióndesdesistemas socio tecnológicoscomplexos. Informatica Salud. 2014;103:21-34.
9. AMD Global Telemedicine. I want to "do telemedicine": What is involved and how much does it cost. Jul 09 2015.
10. Carl HP, Ehsan R, Abtin S, Jay LF. Telemedicine in Ophthalmology: Numerous factors are driving a transition to remote screening. Retina Today. 2017;55-58.
11. Morse AR. Telemedicine in Ophthalmology: Promise and Pitfalls. Ophthalmology. 2014; 121(4):809-11.
12. Zheng Y, He M, Congdon N. The worldwide epidemic of diabetic retinopathy. Indian J Ophthalmol. 2012;60(5):428-31.
13. Statistics about diabetes. American Diabetes Association 2016.. Accessed April 5, 2017.
14. Gupta A, Cavallerano J, Sun JK, Silva PS. Evidence for telemedicine for diabetic retinal diseases. Semin Ophthalmol. 2017;32(1):22-28.
15. Paul Chan RV. Telemedicine diagnostic challenges for ROP. Ophthalmic Digital Health Workshop, University of Illinois, October 2017.
16. Ventura C, Williams SL, Chiang MF. Telemedicine for retinopathy of prematurity diagnosis. In: Yogesan K, Goldschmidt L, Cuadros J, eds. Digital teleretinal screening. Berlin: Springer-Verlag; 2012:169-76.
17. Kelly B. E-Health: Ethical and data privacy challenges in the EU. Informa. 2011 [cited 2015 Feb 4].
18. 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. 1995;281:31-50.

19. Proposal for a Regulation 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 (General Data Protection Regulation)/COM/2012/011 final-2012/0011 (COD).
20. Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations. Official Journal. 1998; 204:37-48.
21. Directive EU 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. Official Journal. 2015; 241:1-15.
22. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal. 2000; 178:1-16.
23. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal. 2002;201:37-47.
24. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. Official Journal. 2011;88:45-65.
25. EHealth Stakeholder Group. Widespread deployment of telemedicines services in Europe. Report of the eHealth Stakeholder Group on implementing the digital agenda for Europe. Key action 13/2 telemedicine version 1.0 final; 12 March 2014.
26. Wood M. Telemedicine and ehealth. NHS European Office; 20 Mar 2015.
27. Kirimlioglu N. "The right to privacy" and the patient views in the context of the personal data protection in the field of health. Biomed Res. 2017,28(4):1464-71.
28. Act of consent; approved by the Italian Ophthalmological Society March 2007 and subsequent amendments. SOI.
29. Charter of fundamental rights of the European Union, 26.10.2012, Official Journal of the European Union, 326/395.
30. Official journal, 12-3-2014, Ordinary supplement n. 20 to Data Storage; General Series n. 59.
31. UNI 11386:2010; Title: Support for Interoperability in the Preservation and Recovery of Digital Objects (SInCRO); ICS: [35.240.30].
32. Duhm J, Fleischmann R, Schmidt S, Hupperts H, Brandt SA. Mobile Electronic Medical Records Promote workflow: Physicians' Perspective from a Survey. JMIR Mhealth Uhealth. 2016;4(2):e70.
33. Fallon EC, Rachel SW, Theodore AS. Impact of the Doctor Patient Relationship. Prim Care Companion CNS Disord. 2015;17(5):10.
34. Hammami MM, Al-Jawarneh Y, Hammami MB, Al Qadire M. Information disclosure in clinical informed consent: "reasonable" patient's perception of norm in high-context communication culture. BMC Med Ethics. 2014;15:3.
35. Observatory of health law; Right of access and privacy in health matters. Valerio Sotte, 2014.
36. Directive NIS2016/1148, Official journal, 09-06-2018,General Series n. 132.
37. eIDAS– Electronic Identification and Signature (Electronic Trust Services) final draft. Certified electronic signature. 2014.
38. Li J. A Privacy Preservation Model for Health-Related Social Networking Sites. J Med Internet Res. 2015;17(7):e168.
39. Decree of the President of the Council of Ministers of 17 February 2017 Directive setting guidelines for cyber protection and national IT security. Official Journal no. 87 of 13 April 2017.
40. Saeta Bruno. Protection and personal data.Bruno Saetta Internet & Diritto; 2018.
41. NIS directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 containing measures for a high common level of security of networks and information systems in the Union; 19.07.2016; EN Official Journal of the European Union.
42. McMenamin JP, Schanz SJ, Storey DD. Regulatory perspectives on telephone-based cross-coverage: Principles for decision-makers. Telehealth Reports (February 2009).